THE MACMILLAN COMPANY
NEW YORK · BOSTON · CHICAGO · DALLAS
ATLANTA · SAN FRANCISCO

MACMILLAN AND CO., LIMITED
LONDON · BOMBAY · CALCUTTA · MADRAS
MELBOURNE

THE MACMILLAN COMPANY
OF CANADA, LIMITED
TORONTO

INTRODUCTION TO THE
THEORY OF EQUATIONS

BY

LOUIS WEISNER, PH.D.

Associate Professor of Mathematics
Hunter College of the City of New York

NEW YORK

THE MACMILLAN COMPANY

1947

Published August, 1938.

Reprinted August, 1947.

PRINTED IN THE UNITED STATES OF AMERICA

PREFACE

The material contained in this book has been presented regularly at Hunter College for the past ten years as a first course in Higher Algebra for students who have completed the introductory courses in the Calculus.

I have made every effort to introduce to the student the spirit of modern algebra, avoiding, however, the emphasis on formalization. The concept of a field dominates the entire work. This concept serves as a great unifying and classifying principle which links together the various topics and makes the Theory of Equations a connected body of doctrine rather than a disjointed set of propositions. I have, however, made no attempt to cultivate all types of fields after the manner of the great work of Steinitz. I have confined myself to fields of characteristic zero and have emphasized particularly those fields which the student for whom this book is designed is equipped to study. At the same time I have anticipated the future needs of the student and the requirements of the more advanced student who should have little difficulty and considerable pleasure in discovering for himself, by an examination of the proofs in the text, to what extent the theorems may be extended to other fields.

The exercises are an essential part of the course. Some are drill problems, but others will tax the ingenuity of the best students. The miscellaneous exercises at the end of the book are provided for further instruction and entertainment.

The book has been used at various times in mimeographed form by my colleagues Professor Marguerite D. Darkow, Professor Mina S. Rees, and Professor Anne Marie Whelan. I am grateful for their helpful suggestions and constructive criticisms.

LOUIS WEISNER

NEW YORK CITY
July, 1938

CONTENTS

CHAPTER I

COMPLEX NUMBERS

CHAPTER II

DIVISION AND FACTORIZATION OF POLYNOMIALS IN A FIELD

CHAPTER III

FURTHER PROPERTIES OF POLYNOMIALS IN A FIELD

CHAPTER IV

THEORY OF EQUATIONS IN THE FIELD OF RATIONAL NUMBERS

CHAPTER V

THEORY OF EQUATIONS IN THE FIELD OF REAL NUMBERS

CHAPTER VI

ELIMINATION. RESULTANTS. SYMMETRIC FUNCTIONS

INTRODUCTION TO THE THEORY OF EQUATIONS

CHAPTER I

COMPLEX NUMBERS

1. Definitions. Operations with complex numbers. Complex numbers arose historically in an effort to solve algebraic equations like

$$x^2 + 1 = 0,$$
$$x^4 + 3x^2 + 1 = 0,$$

which obviously have no real roots. It was found necessary to invent a new number $i = \sqrt{-1}$ which, when combined with real numbers, yielded numbers of the form $a + bi$, where a and b are real numbers. The formal laws of Algebra were assumed to be valid for these complex numbers and the subject developed from that point of view.

We prefer to define the complex number system in terms of the real number system, with which it is assumed that the reader is acquainted. If a and b are real numbers the symbol (a, b) represents an *ordered* pair of real numbers; that is, a pair of real numbers in which order is essential, so that the symbols (a, b) and (b, a) are distinct unless $a = b$. Moreover,

$$(a, b) = (c, d) \tag{1a}$$

if, and only if

$$a = c \text{ and } b = d \tag{1b}$$

Various rules of combination of ordered pairs of real numbers may be, and have been, devised, leading to various algebras of ordered pairs of real numbers, different from one another, but each self-consistent. The complex number system is one of these algebras. The complex number system is the set of all ordered pairs of real

numbers when these ordered pairs are combined according to the rules stated below.

It is convenient at the outset to introduce a special notation for complex numbers. The ordered pair of real numbers (a, b), regarded as a complex number, is written $a + bi$. The symbol i which occurs in this notation is employed to separate the numbers a and b. a is called the *real*, and b the *imaginary*, part of the complex number $a + bi$. It follows from (1) that *two complex numbers are equal if and only if their real parts are equal and their imaginary parts are equal.*

The complex number $a + 0i$ is denoted by a and may, in practice, be identified with the real number a without danger of confusion. In particular $0 = 0 + 0i$ and $1 = 1 + 0i$ are the *zero* and the *unit* respectively of the complex number system. The complex number $0 + bi$, $(b \neq 0)$, is denoted by bi and is called a *pure imaginary number*. In particular $i = 0 + 1i$ is called the *imaginary unit*.

Addition of complex numbers is defined by

$$(2) \qquad (a + bi) + (c + di) = (a + c) + (b + d)i.$$

The symbol $a - bi$ is defined by

$$a - bi = a + (-b)i$$

and hence denotes a complex number. The complex number $-a - bi$ is called the *negative* of $a + bi$ because, as a consequence of the preceding definitions,

$$(a + bi) + (-a - bi) = 0.$$

Following a standard notation, the negative of $a + bi$ is written $-(a + bi)$; hence

$$-(a + bi) = -a - bi.$$

Subtraction of complex numbers is defined by

$$(3) \qquad (a + bi) - (c + di) = (a + bi) + (-(c + di)).$$

The right member is easily reduced to $(a - c) + (b - d)i$.

Multiplication of complex numbers is defined by

$$(4) \qquad (a + bi) \times (c + di) = (ac - bd) + (ad + bc)i.$$

(As usual, multiplication will be indicated by a cross, a dot, or by

mere juxtaposition of the factors.) In particular

$$i^2 = i \times i = -1. \tag{5}$$

With this in mind, the product of two complex numbers may be evaluated by expanding the product according to the formal rules of Algebra and replacing i^2 by -1. Let the student apply this method to the left member of (**4**). Because of (**5**), i is frequently called *the* square root of -1: $i = \sqrt{-1}$. However, $-i$ is also a square root of -1 since $(-i) \times (-i) = -1$ by (**4**).

The complex number $a - bi$ is called the *conjugate imaginary*, or merely the *conjugate*, of $a + bi$; hence $a + bi$ is the conjugate of $a - bi$. By (**4**)

$$(a + bi)(a - bi) = a^2 + b^2,$$

which equals 0 if $a = b = 0$, but is a positive real number otherwise. The positive square root of this product (or 0 when $a = b = 0$) is called the *modulus* or the *absolute value* of $a + bi$ and is written $|a + bi|$; thus

$$|0| = 0; \qquad |a + bi| = +\sqrt{a^2 + b^2}, \qquad (a + bi \neq 0).$$

We readily verify that

$$(a + bi)\left(\frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2}i\right) = 1, \qquad (a + bi \neq 0),$$

and therefore call the second factor of the left member the *reciprocal* of the first. Every complex number different from 0 has a reciprocal. The usual notation is employed for the reciprocal of a complex number; thus

$$\frac{1}{a + bi} = \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2}i, \qquad (a + bi \neq 0).$$

Division of complex numbers is defined by

$$\frac{a + bi}{c + di} = (a + bi) \times \frac{1}{c + di}, \qquad (c + di \neq 0). \tag{6}$$

The ratio may be most conveniently simplified in practice by multiplying the numerator and denominator by the conjugate of the denominator (see Ex. 18 below); thus

$$\frac{2 - 3i}{1 + 4i} = \frac{(2 - 3i)(1 - 4i)}{(1 + 4i)(1 - 4i)} = \frac{-10 - 11i}{17} = -\frac{10}{17} - \frac{11}{17}i.$$

The powers of a complex number are defined as usual:

$$\alpha^1 = \alpha, \quad \alpha^2 = \alpha \times \alpha, \quad \alpha^3 = \alpha^2 \times \alpha, \quad \cdots, \quad \alpha^n = \alpha^{n-1} \times \alpha,$$

where α is a complex number. With the conventions

$$\alpha^0 = 1, \qquad \alpha^{-n} = \frac{1}{\alpha^n}, \qquad (\alpha \neq 0),$$

the laws of exponents

$$\alpha^m \times \alpha^n = \alpha^{m+n}, \qquad \alpha^m \div \alpha^n = \alpha^{m-n}, \qquad (\alpha^m)^n \quad \alpha^{mn},$$

are readily established (see Ex. 13 below).

Other properties of complex numbers will be found among the subjoined exercises. The student who wishes to understand what he is doing should note carefully which of the preceding conventions is applied at each step of the demonstration.

EXERCISES

The Greek letters denote complex numbers.

1. Simplify

(a) $i + 3(1 - i)$.
(b) $(\sqrt{2} + i\sqrt{3}) - (\sqrt{3} - i\sqrt{2})$.
(c) $(a + bi) + (a - bi)$.
(d) $(a + bi) - (a - bi)$.
(e) $(1 + 4i)(2 \quad 3i)$.
(f) $(1 + i)^2$.

2. Simplify

(a) $(2 - i)(1 - 2i)$.
(b) $(2\sqrt{5} - i\sqrt{3})(-\sqrt{3} + 4i\sqrt{5})$.
(c) $-i\sqrt{2}(-3\sqrt{6} - 5i\sqrt{2})$.
(d) $\dfrac{-3 + 4i}{1 - 2i}$.
(e) $1 \div i$.
(f) $\dfrac{(2 + 3i)(5 - 7i)}{(3 - 2i)(-4 + i)}$.

3. Simplify

(a) $\dfrac{\sqrt{7} - i\sqrt{10}}{\sqrt{7} + i\sqrt{10}}$.
(b) i^3.
(c) i^4.
(d) $(1 + i)^3 + (1 - i)^3$.
(e) $(3 - 2i)^4$.
(f) $(\sqrt{3} + i\sqrt{5})^3$.

4. Simplify

(a) $\dfrac{(5 - 6i)^2}{(3 - 4i)^2}$.
(b) $(-\sqrt{2} + i\sqrt{3})^4$.
(c) $\dfrac{}{(-1 + i)(1 - 2i)}$.
(d)
(e) $\dfrac{}{(2 + 5i)^2}$.
(f) $(a + bi)^3 + (a - bi)^3$.

5. Show that 0 is the only complex number which equals its negative.
6. Show that $|a + bi| = |a - bi|$.
7. Show that α, $-\alpha$, $i\alpha$, and $-i\alpha$ have the same absolute values.
8. Show that $|\alpha\beta| = |\alpha||\beta|$.
9. Show that
   (a) $0 + \alpha = \alpha$. (c) $1 \times \alpha = \alpha$.
   (b) $0 \times \alpha = 0$. (d) $(-1) \times \alpha = -\alpha$.
10. Show that $\alpha + \beta = \beta + \alpha$ (Commutative law of addition).
11. Show that $\alpha\beta = \beta\alpha$ (Commutative law of multiplication).
12. Show that $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$ (Associative law of addition).
13. Show that $(\alpha\beta)\gamma = \alpha(\beta\gamma)$ (Associative law of multiplication).
14. Show that $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$ (Distributive law).
15. Show that if $\alpha + \beta = \alpha + \gamma$, then $\beta = \gamma$ (Cancellation law).
16. Show that if $\alpha\beta = \alpha\gamma$, and $\alpha \neq 0$, then $\beta = \gamma$ (Cancellation law).
17. Show that $\frac{\alpha}{\beta} \times \frac{\gamma}{\delta} = \frac{\alpha\gamma}{\beta\delta}$, $(\beta \neq 0, \delta \neq 0)$.
18. Show that $\frac{\alpha\gamma}{\beta\gamma} = \frac{\alpha}{\beta}$, $(\beta \neq 0, \gamma \neq 0)$.
19. Show that the product of two or more complex numbers cannot vanish unless at least one of the factors vanishes.

2. Graphical representation of complex numbers. Addition. The reader will recall that the fundamental concept of Analytic Geometry is that of representing points in a plane by ordered pairs of real numbers (coordinates), so that to each point there corresponds an ordered pair of real numbers, and vice versa. We have seen that a complex number is essentially an ordered pair of real numbers. Hence complex numbers may be represented by the points of a plane.

The complex number $z = x + yi$ is represented graphically by the point whose coordinates are (x, y) with respect to a pair of rectangular axes in a plane. For example, the complex numbers $1 + 2i$, $-1 + 2i$, $-1 - 2i$, $1 - 2i$ are represented by the points $(1, 2)$, $(-1, 2)$, $(-1, -2)$, $(1, -2)$ respectively.

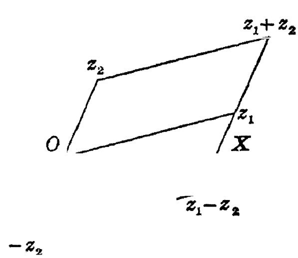

FIG. 1

The x-axis is called the *axis of reals*, as the points on it represent only real numbers; while the y-axis is called the *axis of imaginaries*,

as the points on it represent only pure imaginary numbers. The terms *complex number* and *point* are used interchangeably.

It is readily proved with the aid of the preceding figure that the point $z_1 + z_2$ is the vertex opposite 0 of the parallelogram which has three of its vertices at 0, z_1 and z_2.

To subtract z_2 from z_1 graphically, add z_1 and $-z_2$ as suggested by the figure.

EXERCISES

1. Locate the points representing the following complex numbers: 1, -1, i, $-i$, $\frac{1}{2}(-1 + i\sqrt{3})$, $\frac{1}{2}(-1 - i\sqrt{3})$, $\frac{1}{2}(\sqrt{2} + i\sqrt{2})$, $\frac{1}{2}(\sqrt{2} - i\sqrt{2})$. Show that these points lie on the *unit circle* (a circle of radius 1 with center at the origin).

2. What is the geometric relation between a complex number and (a) its negative? (b) its conjugate?

3. What is the geometric relation between the points z and kz, where k is a real number?

4. How are two complex numbers to be added graphically if the line joining them passes through the origin? Distinguish two cases.

5. Justify the following construction for the point $z_1 - z_2$: Draw a line from z_2 to z_1. From the origin draw a parallel and equal line pointing in the same direction. Its endpoint is $z_1 - z_2$.

6. Perform the indicated operations graphically:
$(1 + i) + (2 + 3i)$, $(-2 + i) + (3 + i)$, $(\sqrt{3} - i) - (\sqrt{2} - i\sqrt{2})$, $(2 + 2i) + (1 - 2i)$, $(-1 - i) - (3 + i)$, $(3 + 2i) + (6 + 4i)$, $(1 - 2i) - (2 - 4i)$, $3 + (-5 - 4i)$, $-4i - (-2 - 6i)$, $-1 - (5 + i)$.

7. Show that the distance from the point z to the origin is $|z|$.

8. Show that the distance between the points z_1 and z_2 is $|z_1 - z_2|$.

9. Show graphically that $|z_1 + z_2| \leq |z_1| + |z_2|$. Generalize.

10. Show graphically that $|z_1 - z_2| \geq ||z_1| - |z_2||$.

11. Show that the points

$$a + bi,\ a - bi,\ -a + bi,\ -a - bi, \qquad (ab \neq 0)$$

are the vertices of a rectangle.

12. Show that the midpoint of the line joining the points z_1 and z_2 is $\frac{1}{2}(z_1 + z_2)$.

13. Show that the centroid (point of intersection of the medians) of the triangle whose vertices are z_1, z_2, and z_3 is $\frac{1}{3}(z_1 + z_2 + z_3)$.

3. Polar form of a complex number. Multiplication. A point in a plane may be represented by its polar coordinates (r, θ) as well as by its cartesian coordinates (x, y). In dealing with polar coordinates

it should be borne in mind that the pairs of numbers

$$(r, \theta + 2k\pi), \qquad (k = 0, \pm 1, \pm 2, \cdots)$$

all represent the same point. We shall take $r \geq 0$. The relations between rectangular and polar coordinates are (see Fig. 2)

$$x = r\cos\theta, \qquad y = r\sin\theta,$$
$$r = \sqrt{x^2 + y^2}, \qquad \theta = \arc\tan\frac{y}{x}.$$

The complex number $z = x + yi$ may now be written

$$z = r(\cos\theta + i\sin\theta),$$

which is known as its *polar* or *trigonometric* form. The number r has already been defined as the modulus or absolute value of z. It is the geometric distance from the point z to the origin and is positive if $z \neq 0$. The angle θ is called the *argument* or *amplitude* of z; we write $\theta = \text{am } z$. The amplitude of every complex number (except 0, which has no amplitude) is multiple-valued, its various values differing by integral multiples of 2π. While any one of these values may be taken as *the* amplitude, preference is frequently given to that value which lies between 0 (inclusive) and 2π (exclusive). In any case, *two complex numbers are equal if, and only if, their moduli are equal and their amplitudes differ by an integral multiple of 2π.*

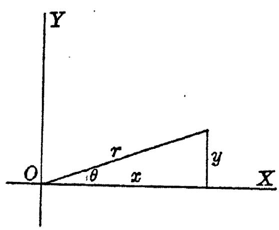

FIG. 2

The polar form of a complex number is convenient for purposes of multiplication or division. The product of the complex numbers

$$z_1 = r_1(\cos\theta_1 + i\sin\theta_1),$$
$$z_2 = r_2(\cos\theta_2 + i\sin\theta_2)$$

is

$$\begin{aligned} z_1z_2 &= r_1r_2[\cos\theta_1\cos\theta_2 - \sin\theta_1\sin\theta_2 + i(\sin\theta_1\cos\theta_2 + \cos\theta_1\sin\theta_2)] \\ &= r_1r_2[\cos(\theta_1 + \theta_2) + i\sin(\theta_1 + \theta_2)], \end{aligned}$$

which is the polar form of z_1z_2. Therefore r_1r_2 and $\theta_1 + \theta_2$ are the modulus and amplitude respectively of z_1z_2. Hence

$$|z_1z_2| = |z_1||z_2|, \qquad \text{am}(z_1z_2) = \text{am } z_1 + \text{am } z_2.$$

The modulus of the product of two complex numbers equals the product of their moduli; and the amplitude of the product of two complex numbers equals the sum of their amplitudes. This theorem tells us how to multiply two complex numbers graphically.

In a similar manner we find that

$$\frac{z_1}{z_2} = \frac{r_1}{r_2}[\cos(\theta_1 - \theta_2) + i \sin(\theta_1 - \theta_2)].$$

Hence

$$\left|\frac{z_1}{z_2}\right| = \frac{|z_1|}{|z_2|} \qquad \text{am}\left(\frac{z_1}{z_2}\right) = \text{am } z_1 - \text{am } z_2.$$

EXERCISES

1. Plot the following complex numbers and write each of them in the polar form, obtaining the modulus and the amplitude directly from the figure: $1,\ -1,\ 3,\ -5,\ 4i,\ -8i,\ -1 + i\sqrt{3},\ \sqrt{3} - i,\ -\sqrt{2} - i\sqrt{2}$, $\frac{1}{2}(\sqrt{2} + i\sqrt{2})$, $\cos 25° - i \sin 25°$, $4(\cos 130° - i \sin 130°)$, $\sin 40° + i \cos 40°$, $-5(\cos 52° + i \sin 52°)$.

2. Plot the following complex numbers and write each of them in the polar form, obtaining the modulus from the figure and the amplitude with the aid of trigonometric tables: $1 + 2i$, $3 - 4i$, $-5 + 12i$, $-1 - i\sqrt{2}$.

3. What is the locus of a point which has (a) a given absolute value? (b) a given amplitude?

4. Simplify, leaving the results in the polar form:

(a) $[3(\cos 10° + i \sin 10°)][\sqrt{2}(\cos 58° + i \sin 58°)]$.

(b) $\left(\cos\frac{\pi}{4} + i \sin\frac{\pi}{4}\right)\left(\cos\frac{\pi}{6} + i \sin\frac{\pi}{6}\right)$.

(c) $\dfrac{(\cos 22° + i \sin 22°)[5(\cos 137° + i \sin 137°)]}{[2(\cos 218° + i \sin 218°)](\cos 98° + i \sin 98°)}$.

5. Show that the points z, iz, $-z$, and $-iz$ are the vertices of a square whose center is 0.

6. Multiply algebraically and graphically:

(a) i by $\frac{1}{2}(-1 - i\sqrt{3})$.

(b) $\frac{1}{2}(\sqrt{2} + i\sqrt{2})$ by $\frac{1}{2}(-1 + i\sqrt{3})$.

(c) $\frac{1}{2}(\sqrt{3} + i)$ by $3 - 4i$.

7. Divide algebraically and graphically:

(a) $2 + i$ by $\dfrac{1 - i}{\sqrt{2}}$.

(b) $-5 + 4i$ by i.

(c) $-i$ by $\frac{1}{2}(1 - i\sqrt{3})$.

8. Show that the reciprocal of $\cos\theta + i \sin\theta$ is $\cos\theta - i \sin\theta$.

9. Under what circumstances are the conjugate and the reciprocal of a complex number equal?

10. Show that $\dfrac{1 + \cos\theta + i\sin\theta}{1 + \cos\theta - i\sin\theta} = \cos\theta + i\sin\theta.$

4. Demoivre's Theorem. From the relation

$$\operatorname{am}(z_1 z_2) = \operatorname{am} z_1 + \operatorname{am} z_2,$$

we readily infer that

$$\operatorname{am}(z_1 z_2 \cdots z_n) = \operatorname{am} z_1 + \operatorname{am} z_2 + \cdots + \operatorname{am} z_n;$$

or

$$(\cos\theta_1 + i\sin\theta_1)(\cos\theta_2 + i\sin\theta_2)\cdots(\cos\theta_n + i\sin\theta_n)$$
$$= \cos(\theta_1 + \theta_2 + \cdots + \theta_n) + i\sin(\theta_1 + \theta_2 + \cdots + \theta_n).$$

Taking $\theta = \theta_1 = \theta_2 = \cdots = \theta_n$, we obtain

$$(\cos\boldsymbol{\theta} + i\sin\boldsymbol{\theta})^n = \cos n\boldsymbol{\theta} + i\sin n\boldsymbol{\theta},$$

where n is any positive integer. This result is known as *Demoivre's Theorem.* This theorem is of great importance in problems dealing with powers or roots of complex numbers. Many useful relations among trigonometric functions may be derived from it.

Example 1. Evaluate $(-1 - i)^{15}$.

Employing the polar form we have $-1 - i = \sqrt{2}(\cos 225° + i\sin 225°)$. Hence

$$\begin{aligned}(-1 - i)^{15} &= 2^{\frac{15}{2}}(\cos 225° + i\sin 225°)^{15} \\ &= 2^{\frac{15}{2}}(\cos 3375° + i\sin 3375°) \\ &= 2^{\frac{15}{2}}(\cos 135° + i\sin 135°) \\ &= 2^{\frac{15}{2}}\left(-\frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}}\right) = 2^7(-1 + i) = -128 + 128i.\end{aligned}$$

Example 2. Deduce two trigonometric identities from the algebraic identity

$$1 + z + z^2 + \cdots + z^{n-1} = \frac{1 - z^n}{1 - z}$$

by substituting $z = \cos\theta + i\sin\theta$.

Making the substitution, we have after employing Demoivre's Theorem,

$$\mathbf{1} + \cos\boldsymbol{\theta} + i\sin\boldsymbol{\theta} + \cos 2\boldsymbol{\theta} + i\sin 2\boldsymbol{\theta} + \cdots + \cos(n - 1)\boldsymbol{\theta}$$
$$+ i\sin(n - 1)\boldsymbol{\theta}$$

$$= \frac{1 - \cos n\theta - i \sin n\theta}{1 - \cos \theta - i \sin \theta}$$

$$= \frac{2 \sin^2 \frac{1}{2}n\theta - 2i \sin \frac{1}{2}n\theta \cos \frac{1}{2}n\theta}{2 \sin^2 \frac{1}{2}\theta - 2i \sin \frac{1}{2}\theta \cos \frac{1}{2}\theta}$$

$$= \frac{\sin \frac{1}{2}n\theta}{\sin \frac{1}{2}\theta} \cdot \frac{\sin \frac{1}{2}n\theta - i \cos \frac{1}{2}n\theta}{\sin \frac{1}{2}\theta - i \cos \frac{1}{2}\theta}$$

$$= \frac{\sin \frac{1}{2}n\theta}{\sin \frac{1}{2}\theta} \cdot \frac{-i(\cos \frac{1}{2}n\theta + i \sin \frac{1}{2}n\theta)}{-i(\cos \frac{1}{2}\theta + i \sin \frac{1}{2}\theta)}$$

$$= \frac{\sin \frac{1}{2}n\theta}{\sin \frac{1}{2}\theta}[\cos \tfrac{1}{2}(n - 1)\theta + i \sin \tfrac{1}{2}(n - 1)\theta].$$

Equating real and imaginary parts, we have

$$1 + \cos \theta + \cos 2\theta + \cdots + \cos (n - 1)\theta = \frac{\sin \frac{1}{2}n\theta \cos \frac{1}{2}(n - 1)\theta}{\sin \frac{1}{2}\theta},$$

$$\sin \theta + \sin 2\theta + \cdots + \sin(n - 1)\theta = \frac{\sin \frac{1}{2}n\theta \sin \frac{1}{2}(n - 1)\theta}{\sin \frac{1}{2}\theta}.$$

EXERCISES

1. Prove that $(\cos \theta - i \sin \theta)^n = \cos n\theta - i \sin n\theta$.

2. Prove Demoivre's Theorem for negative integral values of the exponent.

3. Show that $i^n = \cos \dfrac{n\pi}{2} + i \sin \dfrac{n\pi}{2}$.

4. Show that $(1 + i)^n = 2^{\frac{n}{2}}\left(\cos \dfrac{n\pi}{4} + i \sin \dfrac{n\pi}{4}\right)$. Deduce two relations among binomial coefficients by equating real and imaginary parts.

5. Evaluate

(a) $(1 + i)^{13}$. (c) $\left(\dfrac{1 - i}{\sqrt{2}}\right)^{-11}$. (e) $(-\sqrt{3} - 3i)^{-5}$.

(b) $(\sqrt{3} + i)^{10}$. (d) $(3 - i\sqrt{3})^8$. (f) $\left(\dfrac{-1 - i\sqrt{3}}{2}\right)^{-7}$.

6. Express $\sin 3\theta$ and $\cos 3\theta$ in terms of $\sin \theta$ and $\cos \theta$ by expanding the right member of the identity

$$\cos 3\theta + i \sin 30 = (\cos \theta + i \sin \theta)^3$$

by the binomial theorem.

7. Express similarly $\sin 4\theta$ and $\cos 4\theta$ in terms of $\sin \theta$ and $\cos \theta$.

8. (a) Show that

$$2 \cos \tfrac{1}{2}\theta(\cos \tfrac{1}{2}\theta + i \sin \tfrac{1}{2}\theta) = 1 + (\cos \theta + i \sin \theta).$$

(b) Raise both members of this identity to the nth power, and deduce that

$$1 + \binom{n}{1}\cos\theta + \binom{n}{2}\cos 2\theta + \cdots + \binom{n}{n}\cos n\theta = (2\cos\tfrac{1}{2}\theta)^n \cos\tfrac{1}{2}n\theta,$$

$$\binom{n}{1}\sin\theta + \binom{n}{2}\sin 2\theta + \cdots + \binom{n}{n}\sin n\theta = (2\cos\tfrac{1}{2}\theta)^n \sin\tfrac{1}{2}n\theta,$$

where

$$\binom{n}{r} = \frac{n(n-1)\cdots(n-r+1)}{r!}.$$

9. Substitute $z = \cos\theta + i\sin\theta$ in the identity

$$z + z^3 + z^5 + \cdots + z^{2n-1} = \frac{z - z^{2n+1}}{1 - z^2},$$

and deduce that

$$\cos\theta + \cos 3\theta + \cdots + \cos(2n-1)\theta = \frac{\sin 2n\theta}{2\sin\theta},$$

$$\sin\theta + \sin 3\theta + \cdots + \sin(2n-1)\theta = \frac{\sin^2 n\theta}{\sin\theta}.$$

10. Expand $(x + yi)^n$ and show, by equating the moduli of both members, that

$$(x^2 + y^2)^n = \left[x^n - \binom{n}{2}x^{n-2}y^2 + \binom{n}{4}x^{n-4}y^4 - \cdots\right]^2 + \left[\binom{n}{1}x^{n-1}y - \binom{n}{3}x^{n-3}y^3 + \binom{n}{5}x^{n-5}y^5 - \cdots\right]^2.$$

5. Roots of unity. A *root of unity* is a complex number some power of which equals 1. An nth root of unity is a complex number whose nth power equals 1. If $r(\cos\theta + i\sin\theta)$ is an nth root of unity,

$$r^n(\cos\theta + i\sin\theta)^n = 1;$$

or, by Demoivre's Theorem,

$$r^n(\cos n\theta + i\sin n\theta) = 1.$$

Now the modulus and amplitude of the complex number 1 are 1 and 0 respectively, and two complex numbers are equal if, and only if, their moduli are equal and their amplitudes differ by an integral multiple of 2π. Therefore

$$r = 1, \qquad \frac{2k\pi}{n},$$

k being an integer. All the nth roots of unity are therefore included among the complex numbers

(1) $$\cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}, \qquad (k = 0, \pm 1, \pm 2, \cdots),$$

which are infinite in number but are not all different. However, those nth roots of unity which are included among the complex numbers

$$(2) \qquad \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}, \qquad (k = 0, 1, \cdots, n-1),$$

are certainly distinct as their amplitudes are different and all lie between 0 (inclusive) and 2π (exclusive).

To show that *all* the nth roots of unity are included in (2), we divide the k of (1) by n, obtaining a quotient q and a remainder r satisfying the relation

$$k = qn + r, \qquad (0 \leq r < n).$$

Then

$$\cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n} = \cos\left(2q\pi + \frac{2r\pi}{n}\right) + i\sin\left(2q\pi + \frac{2r\pi}{n}\right)$$
$$= \cos\frac{2r\pi}{n} + i\sin\frac{2r\pi}{n},$$

which is included in (2). The distinct numbers of the set (1) are therefore those of (2). By Demoivre's Theorem the nth power of every number of the set (2) equals 1. We conclude that *there are n distinct nth roots of unity, all of which are given, without repetition, by* (2).

Denoting by ϵ that nth root of unity obtained by taking $k = 1$ in (2); that is,

$$(3) \qquad \epsilon = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n},$$

we have, by Demoivre's Theorem,

$$(4) \qquad \epsilon^k \quad \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n},$$

where k is any integer. *The nth roots of unity are powers of ϵ, the distinct nth roots of unity being*

$$(5) \qquad 1, \epsilon, \epsilon^2, \cdots, \epsilon^{n-1}.$$

Since $|\epsilon^k| = 1$, the points representing the nth roots of unity lie on the unit circle. When the points

$$1, \epsilon, \epsilon^2, \qquad , \epsilon^{n-1}, 1$$

are joined in order by straight lines, a *regular* polygon of n sides is obtained; for the amplitude of

$$\frac{\epsilon^k}{\epsilon^{k-1}} = \epsilon$$

is $2\pi/n$, so that the chord joining the points ϵ^{k-1} and ϵ^k subtends an angle of $2\pi/n$ at the origin.

Fig. 3 exhibits the three cube roots of unity, which are

$$\begin{aligned} \cos 0 \quad + i \sin 0 \quad &= 1, \\ \cos 120^\circ + i \sin 120^\circ &= \tfrac{1}{2}(-1 + i\sqrt{3}), \\ \cos 240^\circ + i \sin 240^\circ &= \tfrac{1}{2}(-1 - i\sqrt{3}). \end{aligned}$$

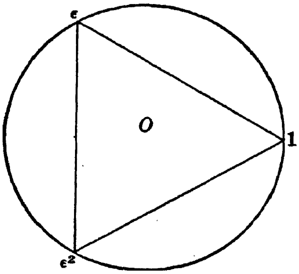

FIG. 3

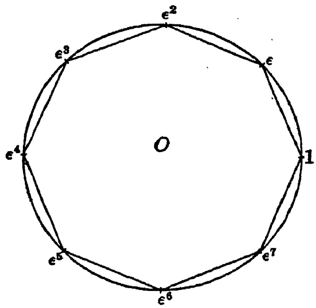

FIG. 4

Fig. 4 exhibits the eight 8th roots of unity, which are

$$\begin{aligned} \cos 0 \quad + \; i \sin 0 \quad &= 1, \\ \cos 45^\circ + \; i \sin 45^\circ &= \tfrac{1}{2}(\sqrt{2} + i\sqrt{2}), \\ \cos 90^\circ + \; i \sin 90^\circ &= i, \\ \cos 135^\circ + i \sin 135^\circ &= \tfrac{1}{2}(-\sqrt{2} + i\sqrt{2}), \\ \cos 180^\circ + i \sin 180^\circ &= -1, \\ \cos 225^\circ + i \sin 225^\circ &= \tfrac{1}{2}(-\sqrt{2} - i\sqrt{2}), \\ \cos 270^\circ + i \sin 270^\circ &= -i, \\ \cos 315^\circ + i \sin 315^\circ &= \tfrac{1}{2}(\sqrt{2} - i\sqrt{2}). \end{aligned}$$

EXERCISES

1. Show directly from the definition of nth root of unity that

(a) the product of two nth roots of unity is an nth root of unity.

(b) the reciprocal of an nth root of unity is an nth root of unity.

2. Show that -1 is an nth root of unity if and only if n is even.

3. Simplify i^{13}, i^{95}, i^{-22}, i^{-52}, i^{1000}. [Write the exponent in the form $4q + r$, where $r = 0, 1, 2$, or 3. Then $i^{4q+r} = i^{4q}i^r = i^r$, since $i^{4q} = 1$.]

4. Show that $\frac{1}{4}(1 + i^n + i^{2n} + i^{3n})$ assumes the value 1 if n is divisible by 4, and the value 0 otherwise.

5. What values does $\dfrac{1}{2i}(i^n - i^{-n})$ assume for integral values of n?

6. Simplify ω^{10}, ω^{71}, ω^{-62}, ω^{-85}, ω^{15}, where ω is an imaginary cube root of unity.

7. What values does $\frac{1}{3}(1 + \omega^n + \omega^{2n})$ assume for integral values of n?

8. Simplify ϵ^{19}, ϵ^{-62}, ϵ^{91}, ϵ^{100}, ϵ^{42}, where ϵ is an imaginary 5th root of unity.

9. Show that the sum of the nth roots of unity is 0 if $n \geq 2$. [Use (**5**).]

10. Show that if $n \geq 2$, the sum of the kth powers of the nth roots of unity is n if k is divisible by n, and 0 otherwise.

11. Show that the product of all the nth roots of unity is $+1$ if n is odd and -1 if n is even. [Use (**5**) and (**4**).]

12. Show that if z is any complex number different from 0, and $\epsilon = \cos\dfrac{2\pi}{n} + i\sin\dfrac{2\pi}{n}$, $(n \geq 3)$, the points z, ϵz, $\epsilon^2 z$, [illegible]^{-1}z are the vertices of a regular polygon of n sides.

13. Show that $| 1 - \epsilon^k | = 2\sin\dfrac{k\pi}{n}$.

14. Plot the 4th, 6th, and 12th roots of unity, and express them in a form free from trigonometric functions.

15. In Fig. 5, $AC = BC = 1$, $AB = CD = BD = x$, the angles being indicated in the figure.

(a) Find the value of x with the aid of a pair of similar triangles.

(b) Find $\cos 72°$ and $\sin 72°$.

(c) Plot the five 5th roots of unity and express them in terms of radicals.

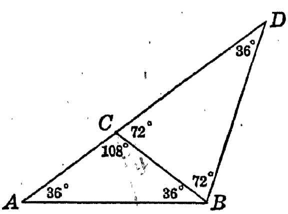

FIG. 5

6. Primitive nth roots of unity. An nth root of unity which is not also an rth root of unity $(r < n)$ is called a *primitive* nth root of unity.

Referring to the 8th roots of unity listed in § 5, we observe that 1, -1, i, and $-i$ are also 4th roots of unity and hence are not primitive 8th roots of unity. With the notation $\epsilon = \cos 2\pi/8 + i\sin 2\pi/8$, the primitive 8th roots of unity are ϵ, ϵ^3, ϵ^5, and ϵ^7, and each of these four exponents is prime to 8. On the other hand, $\epsilon^2 = i$ and $\epsilon^6 = -i$ are primitive 4th roots of unity and each of

these two exponents has the g.c.d. (greatest common divisor) 2 with 8. These remarks serve to illustrate the following theorem.

THEOREM. *If d is the g.c.d. of k and n, then ϵ^k is a primitive n/d th root of unity, where* $\epsilon \quad \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}$.

From the relation

$$\epsilon^r = \cos \frac{2r\pi}{n} + i \sin \frac{2r\pi}{n}$$

we infer that $\epsilon^r = 1$ when and only when r is divisible by n. This statement holds even when $r = 0$, as 0 is divisible by every integer except itself.

With the notation stated in the theorem,

$$(\epsilon^k)^{n/d} = \epsilon^{kn/d} = (\epsilon^n)^{k/d} = 1,$$

since $\epsilon^n = 1$ and k/d is an integer. Therefore ϵ^k is certainly an n/dth root of unity, and it only remains to show that it is a *primitive* n/dth root of unity.

Suppose that $(\epsilon^k)^r = 1$, $(r \neq 0)$, so that $\epsilon^{kr} = 1$. Then kr is divisible by n, and $(k/d) \cdot r$ is divisible by n/d. Since d is the *greatest* common divisor of k and n, k/d and n/d are relatively prime. Since $(k/d) \cdot r$ is divisible by n/d, and k/d and n/d are relatively prime, r must be divisible by n/d. The *smallest* positive integer r for which $(\epsilon^k)^r = 1$ is therefore $r = n/d$. We conclude that ϵ^k is a primitive n/dth root of unity.

COROLLARY 1. *Of the n nth roots of unity*

$$\epsilon^0 = 1, \epsilon, \epsilon^2, \qquad , \epsilon^{n-1},$$

the primitive nth roots of unity are those, and only those, whose exponents are prime to n.

For, in order that ϵ^k be a primitive nth root of unity, it is necessary and sufficient that the g.c.d. of k and n be 1.

COROLLARY 2. *If λ is any primitive nth root of unity, and d is the g.c.d. of k and n, then λ^k is a primitive n/d th root of unity.*

By Corollary 1, $\lambda = \epsilon^l$, where l is prime to n. Hence $\lambda^k = \epsilon^{kl}$. Since the g.c.d. of kl and n is the same as the g.c.d. of k and n, namely d, λ^k is a primitive n/dth root of unity.

EXERCISES

1. Show that the reciprocal of a primitive nth root of unity is a primitive nth root of unity.

2. How many primitive nth roots of unity are there for $n = 4, 5, 6, 12, 15, 18, 20$?

3. How many primitive pth roots of unity are there if p is a prime number? How many primitive p^2th roots of unity?

4. Show that if c is prime to n, the first n powers of ϵ^c are the distinct nth roots of unity; and that this is *not* the case if c is not prime to n. In other words, if λ is an nth root of unity, the first n powers of λ are the distinct nth roots of unity if, and only if, λ is a *primitive* nth root of unity.

5. Let ϵ be a primitive 15th root of unity.

(a) Which of the first 15 powers of ϵ are primitive 15th roots of unity?

(b) Which are primitive 5th roots of unity?

(c) Which are primitive cube roots of unity?

(d) The only remaining 15th root of unity is 1 (a primitive first root of unity).

6. Classify similarly the 9th roots of unity, placing the primitive dth roots of unity in the same class, where $d = 1, 3$, and 9.

7. Classify similarly the nth roots of unity for $n = 6, 10$, and 12.

8. Show that all the dth roots of unity satisfy the equation $x^n = 1$ (and hence are also nth roots of unity) if, and only if, d is a divisor of n.

9. Show that the common roots of the equations

$$x^n = 1, \qquad x^m = 1$$

are the roots of $x^d = 1$, where d is the g.c.d. of n and m.

10. Show that if $d_1, d_2, \cdots, d_r$ are the distinct positive divisors of n, including 1 and n, then the distinct primitive d_jth roots of unity, where $j = 1, 2, \cdots, r$, constitute, without repetition, the distinct nth roots of unity. Exercises 5, 6, and 7 furnish illustrations.

7. Roots of complex numbers. A complex number z satisfying the equation $z^n = w$, where w is a given complex number, is called an nth root of w. The only solution of the equation $z^n = 0$ is $z = 0$. We shall suppose hereafter, in treating the equation $z^n = w$, that $w \neq 0$.

Writing w in the polar form $w = \rho(\cos\varphi + i\sin\varphi)$, we have the equation

$$z^n = \rho(\cos\varphi + i\sin\varphi).$$

If $z = r(\cos\theta + i\sin\theta)$ is a root of this equation,

$$r^n(\cos n\theta + i\sin n\theta) = \rho(\cos\varphi + i\sin\varphi).$$

Therefore, as the moduli of two equal complex numbers are equal

while their amplitudes differ by an integral multiple of 2π,

$$r = \sqrt[n]{\rho}, \quad \theta = \frac{\varphi + 2k\pi}{n},$$

where $\sqrt[n]{\rho}$ denotes the *positive real* nth root of ρ, and k is an integer. Conversely, by Demoivre's Theorem, if k is any integer,

$$z_k = \sqrt[n]{\rho}\left[\cos\left(\frac{\varphi}{n} + \frac{2k\pi}{n}\right) + i \sin\left(\frac{\varphi}{n} + \frac{2k\pi}{n}\right)\right]$$

is an nth root of w. As in § 5, there are only n distinct nth roots of w, obtained by taking $k = 0, 1, \cdots, n - 1$. Moreover, these roots are the vertices of a regular polygon of n sides inscribed in a circle whose radius is $\sqrt[n]{\rho}$, and whose center is 0.

Example 1. Find the three cube roots of $\frac{1}{2}(\sqrt{2} + i\sqrt{2})$.

We first write the number in the polar form:

$$\tfrac{1}{2}(\sqrt{2} + i\sqrt{2}) = \cos 45^\circ + i \sin 45^\circ.$$

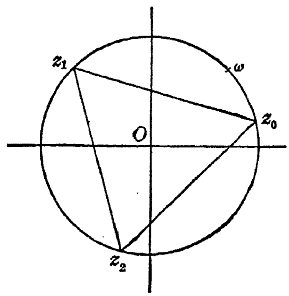

FIG. 6

In the adjacent figure this complex number is marked w. Trisecting the amplitude of w, the point z_0 is located on the unit circle. The other cube roots of w are found by adding 120° and 240° to the amplitude of z_0. They are marked z_1 and z_2 in the figure. This completes the graphical solution, which shows that the three roots are

$$\begin{aligned} z_0 &= \cos\ 15^\circ + i \sin\ 15^\circ \quad \tfrac{1}{4}(\sqrt{6} + \sqrt{2}) + \frac{i}{4}(\sqrt{6} - \sqrt{2}), \\ z_1 &= \cos 135^\circ + i \sin 135^\circ = \tfrac{1}{2}(-\sqrt{2} + i\sqrt{2}), \\ z_2 &= \cos 255^\circ + i \sin 255^\circ = -\tfrac{1}{4}(\sqrt{6} - \sqrt{2}) - \frac{i}{4}(\sqrt{6} + \sqrt{2}). \end{aligned}$$

Example 2. Find the five 5th roots of $3 + 4i$.

We find, with the aid of trigonometric tables that

$$3 + 4i = 5(\cos 53^\circ\, 7.8' + i \sin 53^\circ\, 7.8').$$

The modulus of each fifth root is $\sqrt[5]{5} = 1.3797$. The amplitude of one fifth root is $\dfrac{53^\circ\, 7.8'}{5} = 10^\circ\, 37.5'$. The amplitudes of the other roots are obtained by adding 72°, 144°, 216°, and 288° to 10° 37.5′.

The required roots are therefore (to the indicated degree of accuracy)

$$
\begin{aligned}
z_0 &= \sqrt[5]{5}(\cos 10^\circ\, 37.5' + i \sin 10^\circ\, 37.5') \\
&= 1.3797(.98285 + .18438i) = 1.3560 + .2544i, \\
z_1 &= \sqrt[5]{5}(\cos 82^\circ\, 37.5' + i \sin 82^\circ\, 37.5') \\
&= 1.3797(.12836 + .99174i) = .1771 + 1.3683i, \\
z_2 &= \sqrt[5]{5}(\cos 154^\circ\, 37.5' + i \sin 154^\circ\, 37.5') \\
&= 1.3797(-.90352 + .42854i) = -1.2466 + .5913i, \\
z_3 &= \sqrt[5]{5}(\cos 226^\circ\, 37.5' + i \sin 226^\circ\, 37.5') \\
&= 1.3797(-.68677 - .72687i) = -.9475 - 1.0029i, \\
z_4 &= \sqrt[5]{5}(\cos 298^\circ\, 37.5' + i \sin 298^\circ\, 37.5') \\
&= 1.3797(.47908 - .87777i) = .6610 - 1.2111i.
\end{aligned}
$$

The fact that the sum of all the roots is 0 (see Ex. 2 below) serves as a useful check.

EXERCISES

1. If z_0 is one root of the equation $z^n = w$, $(w \neq 0)$, and ϵ is a primitive nth root of unity, show that the other roots are $z_0\epsilon, z_0\epsilon^2, \cdots, z_0\epsilon^{n-1}$, (which are distinct by Ex. 4, p. 16).

2. Show that the sum of the roots of the equation $z^n = w$, $(n \geq 2)$, is 0.

3. Verify the theorem of Ex. 1 by showing that

$$z_1 = \tfrac{1}{2}(-1 + i\sqrt{3})z_0, \qquad z_2 = \tfrac{1}{2}(-1 - i\sqrt{3})z_0,$$

where z_0, z_1, z_2 are the results of Example 1 of the text.

4. Find the square roots of i, $-i$, $\frac{1}{2}(-\sqrt{2} + i\sqrt{2})$, $\frac{1}{2}(-1 - i\sqrt{3})$, $\sqrt{3} + i$, $3 - i\sqrt{3}$.

5. Find real numbers A and B such that $\sqrt{a + bi} = A + Bi$, $a + bi$ being a given complex number.

6. Solve the quadratic equation

$$ax^2 + bx + c = 0, \qquad (a \neq 0),$$

by the method of completing the square, showing that the usual formula is valid if a, b, and c are complex numbers.

7. Solve the quadratic equations

(a) $x^2 + (1 - 2i)x + 1 - 7i = 0.$ *Ans.* $x = 1 + 3i, -2 - i.$

(b) $x^2 - (6 + i)x + 5 + 5i = 0.$

(c) $x^2 - 2x + 4 + 4i = 0.$

(d) $x^2 - 2ix - 10 = 0.$

8. Find the four 4th roots of 81, -25, $\frac{1}{2}(-1 - i\sqrt{3})$, $-1 + i\sqrt{3}$, $-i$, $16i$.

9. Find the three cube roots of -1, i, $-i$, $\dfrac{-1-i}{\sqrt{2}}$, $1-i$, $2+2i$.

10. Solve

(a) $z^3 = 2 - 3i$, (b) $z^4 = 5 + 2i\sqrt{14}$,

by the method of Example 2.

11. Show that the roots of the cubic equation

$$a_0z^3 + a_1z^2 + a_2z + a_3 = 0, \qquad (a_0 \neq 0),$$

are the vertices of an equilateral triangle if, and only if $3a_0a_2 - a_1^2 = 0$. $\left[\text{Transform the equation by the substitution } z = z' - \dfrac{a_1}{3a_0}.\right]$

12. Show that the roots of the equation

$$z^4 + 4iz^3 - 6z^2 - 4iz - i = 0$$

are the vertices of a square. [Substitute $z = z' - i$.]

CHAPTER II

DIVISION AND FACTORIZATION OF POLYNOMIALS IN A FIELD

8. Number-fields. A set of complex numbers is called a *field*, or, more specifically, a *number-field*, if the set contains at least two distinct numbers, and the sum, difference, product, and quotient of any two numbers of the set is in the set, division by 0 being always excluded. The numbers of the field are called its *elements.*

Example 1. The rational numbers form a field; for the sum, difference, product, and quotient of any two rational numbers is a rational number.

Example 2. The real numbers form a field.

Example 3. The complex numbers form a field.

Example 4. The numbers of the form $a + b\sqrt{2}$, where a and b range independently over the field of rational numbers, form a field:

$$(a_1 + b_1\sqrt{2}) \pm (a_2 + b_2\sqrt{2}) = a_1 \pm a_2 + (b_1 \pm b_2)\sqrt{2};$$

$$(a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2}) = a_1a_2 + 2b_1b_2 + (a_1b_2 + a_2b_1)\sqrt{2};$$

$$\frac{1}{a + b\sqrt{2}} = \frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2}.$$

Since $\sqrt{2}$ is an irrational number, $a^2 - 2b^2 \neq 0$ unless $a = b = 0$. The reciprocal of every number of the set, except 0, is therefore in the set. Finally,

$$\frac{a_1 + b_1\sqrt{2}}{a_2 + b_2\sqrt{2}} = (a_1 + b_1\sqrt{2}) \cdot \frac{1}{a_2 + b_2\sqrt{2}},$$

from which it follows that the quotient of two numbers of the set is in the set.

Example 5. The numbers of the form $a + b\sqrt[3]{2} + c\sqrt[3]{4}$, where a, b, and c range independently over the field of rational numbers, form a field. The only difficulty in proving this statement is in showing that the reciprocal of any number of the set is in the set. For this purpose we form the cubic equation with rational coeffi-

cients, of which $x = a + b\sqrt[3]{2} + c\sqrt[3]{4}$ is a root. We have, after transposing a and cubing both members,

$$\begin{aligned} x^3 - 3ax^2 + 3a^2x - a^3 &= 2b^3 + 6b^2c\sqrt[3]{2} + 6bc^2\sqrt[3]{4} + 4c^3 \\ &= 2b^3 + 6bc(b\sqrt[3]{2} + c\sqrt[3]{4}) + 4c^3 \\ &= 2b^3 + 6bc(x - a) + 4c^3. \end{aligned}$$

The required cubic equation is therefore

$$x^3 - 3ax^2 + (3a^2 - 6bc)x - (a^3 + 2b^3 + 4c^3 - 6abc) = 0.$$

If $a^3 + 2b^3 + 4c^3 - 6abc = 0$, and $x \neq 0$, then x satisfies the quadratic equation

$$x^2 - 3ax + 3a^2 - 6bc = 0.$$

Substituting in this equation

$$\begin{aligned} x &= a + b\sqrt[3]{2} + c\sqrt[3]{4}, \\ x^2 &= a^2 + 4bc + (2c^2 + 2ab)\sqrt[3]{2} + (b^2 + 2ac)\sqrt[3]{4}, \end{aligned}$$

we have

$$a^2 - 2bc + (2c^2 - ab)\sqrt[3]{2} + (b^2 - ac)\sqrt[3]{4} = 0.$$

We shall prove later that $\sqrt[3]{2}$ does not satisfy a linear or quadratic equation with rational coefficients. Assuming this to be the case, we have

$$a^2 - 2bc = 0, \qquad 2c^2 - ab = 0, \qquad b^2 - ac = 0.$$

Eliminating c from the first and third of these equations, we have $a^3 = 2b^3$, from which it follows that $\sqrt[3]{2}$ is a rational number. This is not true. Therefore if $x \neq 0$, $a^3 + 2b^3 + 4c^3 - 6abc \neq 0$.

Dividing the equation

$$x^3 - 3ax^2 + (3a^2 - 6bc)x = a^3 + 2b^3 + 4c^3 - 6abc$$

by x, etc., we obtain

$$\frac{1}{x} = \frac{x^2 - 3ax + 3a^2 - 6bc}{a^3 + 2b^3 + 4c^3 - 6abc}.$$

We conclude that the reciprocal of every number of the set, except 0, is in the set.

It follows from the definition of *field* that any finite number of *rational operations*—the rational operations are addition, subtraction, multiplication, and division—performed on a finite number

of numbers of a field yield a number which is in the field. This property is briefly expressed by the statement: a field is *closed* with respect to the rational operations.

The symbol $R(a_1, a_2, \cdots)$ denotes the smallest field containing the numbers $a_1, a_2, \cdots$. It consists of all numbers which can be obtained by performing a finite number of rational operations on the numbers $a_1, a_2, \cdots$. The field is said to be *generated* by the numbers $a_1, a_2, \cdots$, which are called *generators* of the field.

Example 6. The field $R(1)$, generated by the number 1, is the field of rational numbers. For, a field which contains 1 must also contain

$$2 = 1 + 1, 3 = 2 + 1, \cdots,$$
$$0 = 1 - 1, -1 = 0 - 1, -2 = 0 - 2, \cdots.$$

The field therefore contains every rational number and evidently contains no irrational number.

Example 7. $R(\sqrt{2})$ is the field consisting of the numbers of the form $a + b\sqrt{2}$, where a and b are rational numbers. For, a field which contains $\sqrt{2}$ must also contain $\sqrt{2}/\sqrt{2} = 1$. It therefore contains all the rational numbers (Example 6). The field also contains $b\sqrt{2}$, where b is any rational number, and therefore also $a + b\sqrt{2}$, where a and b are any rational numbers. No other numbers can be obtained by rational operations on $\sqrt{2}$. As the numbers of the form $a + b\sqrt{2}$ form a field (Example 4), this field is the smallest which includes $\sqrt{2}$.

EXERCISES

1. Show that the following sets of numbers are not fields:

(a) The integers $0, 1, 2, \cdots$.

(b) The rational numbers $\leq 10{,}000$.

(c) The numbers of the form $b\sqrt{2}$, (b rational).

(d) $1, -1, i, -i$.

(e) 0.

(f) The numbers of the form $a + b\sqrt{2} + c\sqrt{3} + d\sqrt{5}$, where a, b, c, and d are rational numbers.

(g) The numbers of the form $a + b\sqrt[3]{3}$, where a and b are rational numbers.

2. What are the numbers of the following fields?

(a) $R(\sqrt[3]{2})$.	(d) $R(-i)$.	(g) $R(i, \sqrt{2})$.
(b) $R(\sqrt[4]{5})$.	(e) $R(\sqrt{2}, \sqrt{3})$.	(h) $R(i, i\sqrt{5})$.
(c) $R(i)$.	(f) $R(\sqrt{2}, \sqrt{-3})$.	(i) $R(14)$.

3. Find the reciprocal of

(a) $7 + 2\sqrt[3]{2}$. (b) $1 + \sqrt[3]{3}$. (c) $\sqrt[3]{5} + \sqrt[3]{25}$.

4. Simplify

(a) $\dfrac{2 + \sqrt[3]{9}}{1 + \sqrt[3]{3}}$ (b) $\dfrac{\sqrt[3]{2}}{1 + \sqrt[3]{2} + \sqrt[3]{4}}$

5. Show that every number-field contains all the rational numbers.

6. Show that $R(\sqrt{2}, \sqrt{3}) = R(\sqrt{2}, \sqrt{6}) = R(\sqrt{3}, \sqrt{6})$. (Naturally, two fields are said to be *equal* if they consist of the same numbers.)

7. Show that if α is an element of $R(\beta)$, then every element of $R(\alpha)$ is an element of $R(\beta)$.

8. Show that if α is an element of $R(\beta)$, and β is an element of $R(\alpha)$, then $R(\alpha) = R(\beta)$.

9. Show that $\sqrt{2}$ is not an element of $R(\sqrt{3})$. [Show that an equation of the form $\sqrt{2} = a + b\sqrt{3}$, where a and b are rational numbers, is impossible.]

10. Show that i is not an element of $R(\sqrt{-3})$.

9. Fields of rational functions. The function

$$\frac{a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n}{b_0x^m + b_1x^{m-1} + \cdots + b_{m-1}x + b_m}$$

is called a *rational* function of x *in* a field R if the a's and b's are elements of R and at least one of the b's is different from 0. It is assumed that the reader is acquainted with the rules of combination of rational functions. It is an immediate consequence of these rules that the set of all rational functions in a field is closed with respect to the rational operations; that is, the sum, difference, product, and quotient of two rational functions in a field are rational functions in that field. For this reason the set of all rational functions of a variable x in a field R is called a *field*. This field is denoted by $R(R, x)$ or by $R(x)$. The elements of R are elements of $R(x)$ and are called *constants* with respect to the field $R(x)$.

Similarly, the set of all rational functions, with coefficients in a field R, of several independent variables $x_1, x_2, \cdots, x_p$ not contained in R, form a field denoted by $R(R, x_1, x_2, \cdots, x_p)$ or by $R(x_1, x_2, \cdots, x_p)$.

The term *field* is applied to any class consisting of at least two elements, for which suitable definitions of the rational operations have been set up so that the formal rules of Algebra are valid (such as the commutative, associative, and distributive laws), and which is closed with respect to the rational operations as defined. While

we shall confine our attention in this book exclusively to number-fields, fields of rational functions and certain other fields derived from these fields, it may interest the reader to know that other fields exist. There are fields whose elements are irrational functions of one or more variables, fields whose elements are themselves classes of numbers, fields whose elements are symbols which are combined according to certain formal rules. Should the reader become acquainted with such fields he will find that the theorems proved in this chapter, and many of the theorems proved in subsequent chapters, are valid in all fields.

10. Polynomials in a field. The function

$$A(x) = a_0x^n + a_1x^{n-1} + \qquad + a_{n-1}x + a_n$$

is called a *rational integral function* or a *polynomial in* a field R if all its coefficients $a_0, \cdots, a_n$ are elements of R and R does not include the variable x.* Under the same circumstances $A(x) = 0$ is an equation *in* the field R. It will be noticed that $A(x)$ involves no negative or fractional powers of x.

If $a_0 \neq 0$, the polynomial $A(x)$ and the equation $A(x) = 0$ are of *degree n*; a_0 is the *leading coefficient* and a_n the *final coefficient* or *constant term* of the polynomial as well as of the equation. Every element of R, except 0, is a polynomial in R of degree 0. 0 is also a polynomial in R, but without any degree; it is called the *zero-polynomial.* The elements of R, regarded as polynomials, are called *constants.*

Two polynomials are *equal* if they are identical; that is, if their degrees are equal, and coefficients of like powers of the variable are equal.

If the equation $A(x) = 0$ is satisfied by $x = \alpha$, α is a *root* of the polynomial $A(x)$ and of the equation $A(x) = 0$. The root may or may not be an element of the field R. When R is a number-field the equation $A(x) = 0$ is called an *algebraic equation.*

The function of $m \geq 2$ variables

$$F(x_1, \cdots, x_m) = f_0(x_1, \cdots, x_{m-1})x_m^n + f_1(x_1, \cdots, x_{m-1})x_m^{n-1} + \cdots + f_{n-1}(x_1, \cdots, x_{m-1})x_m + f_n(x_1, \cdots, x_{m-1})$$

is called a *rational integral function* or a *polynomial in* a field R if the coefficients of the powers of x_m are polynomials in $x_1, \cdots, x_{m-1}$ with coefficients in R. This is an example of a definition by

* This means that R does not contain rational functions of x.

induction. A polynomial in one variable having been defined, the preceding definition applies to a polynomial in two variables; now that we know the meaning of a polynomial in two variables, the definition applies to a polynomial in three variables; etc.

If $f_0(x_1, \cdots, x_{m-1}) \neq 0$, n is the *degree* of $F(x_1, \cdots, x_m)$ in x_m. Since the terms of $F(x_1, \cdots, x_m)$ may be arranged according to powers of any one of the variables $x_1, \cdots, x_m$, the polynomial has a degree in *each* of these variables. The polynomial also has a degree in *all* the variables. We may write the polynomial in the expanded form

$$F(x_1, \qquad , x_m) = \Sigma c_{q_1 q_2 \cdots q_m} x_1^{q_1} x_2^{q_2} \cdots x_m^{q_m},$$

where $c_{q_1 q_2 \cdots q_m} \neq 0$ is an element of R. The degree of the monomial $x_1^{q_1} x_2^{q_2} \cdots x_m^{q_m}$ is $q_1 + q_2 + \cdots q_m$. The degree of $F(x_1, \cdots, x_m)$ in all the variables is the largest of the integers $q_1 + q_2 + \cdots + q_m$. If $q_1 + q_2 + \cdots + q_m$ has the same value for each term of the expanded form of the polynomial, $F(x_1, \cdots, x_m)$ is called a *homogeneous* function of $x_1, \cdots, x_m$.

In the following sections we shall deal with a polynomial in one variable with coefficients in a field R. This field may be a number-field or a field of rational functions. In particular, the polynomial may be a function of several variables in which a special prerogative has been assigned to one of the variables.

11. The division algorithm. Given two polynomials $A(x)$ and $B(x) \neq 0$, the reader knows how to divide the first by the second, the object of the division being to obtain a quotient $Q(x)$ and a remainder $S(x)$ satisfying the relation

$$A(x) = Q(x)B(x) + S(x); \tag{1}$$

the remainder, if not 0, being a polynomial whose degree is less than that of the divisor $B(x)$. If $S(x) = 0$, $A(x)$ is *divisible* by $B(x)$ and is a *multiple* of $B(x)$; while $B(x)$ is a *divisor* or a *factor* of $A(x)$. It is not our intention to review the method of dividing one polynomial by another. There are, however, three important points relating to the division algorithm which must be emphasized.

First, the division algorithm involves only *rational* operations on the coefficients of the dividend and divisor. If, for example, the coefficients of the dividend and divisor are rational numbers, no irrational numbers can be introduced in the course of the division;

the coefficients of the quotient and remainder are therefore also rational numbers. More generally, *if the dividend and divisor are in a field R, so are the quotient and remainder.*

Secondly, the result of the division expressed by (**1**) is an *algebraic identity.* (**1**) means that, on multiplying $Q(x)$ by $B(x)$ and adding $S(x)$, where x is a *variable,* $A(x)$ is obtained. Therefore (**1**) is satisfied by *every* complex number x and remains valid if x is replaced by any function of x. An *equation,* however, is not satisfied by every value of the unknown. For example, $x^2 - 1 = 0$ is an algebraic equation satisfied only by $x = 1$ and $x = -1$; while $x^2 - 1 = (x - 1)(x + 1)$ is an algebraic identity. (Compare with the distinction between trigonometric *equations* like $\sin\theta = \frac{1}{2}$ and trigonometric *identities* like $\sin^2\theta + \cos^2\theta = 1$.)

Thirdly, the quotient and remainder are *unique.* For, suppose we also had

$$A(x) = Q_1(x)B(x) + S_1(x),$$

where $Q_1(x)$ and $S_1(x)$ are polynomials and $S_1(x)$, if not 0, has a degree less than that of $B(x)$. Subtracting this equation from (**1**), we have

$$B(x)[Q(x) - Q_1(x)] = S_1(x) - S(x).$$

If $Q(x) \not\equiv Q_1(x)$, this equation involves an absurdity as the left member is a polynomial whose degree is greater than that of the right member. Therefore $Q(x) = Q_1(x)$ and $S(x) = S_1(x)$.

The preceding results are summarized in the

THEOREM 1. *If $A(x)$ and $B(x) \not\equiv 0$ are polynomials in a field R, there exist two unique polynomials $Q(x)$ and $S(x)$ in R satisfying the algebraic identity in x*

$$A(x) = Q(x)B(x) + S(x).$$

If $S(x) \not\equiv 0$, its degree is less than that of $B(x)$.

EXERCISES

1. Which of the following functions are polynomials? Which are rational functions?

(a) x^3. (d) 7. (g) $\frac{1}{2}x^4 - \frac{7}{5}x^3 + \frac{4}{3}x^2 - x + 8$.

(b) x^{-3}. (e) $\frac{17}{21}$. (h) $x^2 - \sqrt{3}x^{-1}$.

(c) $\frac{1}{x}$. (f) $\frac{2x - \sqrt{10}}{3x + 2i}$. (i) $x^3 + 5tx^2 - \frac{6(t + 1)x}{t} + \frac{t - 9}{t^2 + 1}$.

2. (a) Is the polynomial $3x - 3$ a divisor of the polynomial $x - 1$?
(b) Is the polynomial $\frac{1}{2}x - \frac{2}{3}$ divisible by the polynomial 3?
(c) Is the polynomial 3 a divisor of the polynomial 5?
(d) Is the polynomial $\frac{3}{5}$ divisible by the polynomial $-\frac{7}{4}$?
(e) In the field $R(t)$, is the polynomial t^2x a divisor of the polynomial tx^2?

3. Show that if the product of two or more polynomials is the zero-polynomial, one of the factors is the zero-polynomial.

4. Show that the degree of the product of two or more polynomials, none of which is the zero-polynomial, is equal to the sum of the degrees of the factors.

5. Show that if A, B, and C are polynomials, and

$$AB = AC \qquad (A \neq 0),$$

then $B = C$.

6. Show that if each of two polynomials in R is divisible by the other, their ratio is an element of R different from zero.

DEFINITION: Two such polynomials are *associates* in R.

7. Show that if A is divisible by B, and B is divisible by C, then A is divisible by C.

8. Show that if D is a divisor of A and of B, then D is a divisor of $VA + UB$, U and V being arbitrary polynomials.

9. Prove the *Remainder Theorem: The remainder obtained when the polynomial* $A(x)$ *is divided by the polynomial* $x - r$ *is* $A(r)$, r *being a constant.* [Use Theorem 1, with $B(x) = x - r$.]

10. Prove the *Factor Theorem: The polynomial* $A(x)$ *is divisible by the polynomial* $x - r$ *if, and only if,* $A(r) = 0$.

11. Show that $x^n - y^n$ is divisible by $x - y$.

12. Show that $x^3 + y^3 + z^3 - 3xyz$ is divisible by $x + y + z$.

13. Show that $xy^n + yz^n + zx^n - x^ny - y^nz - z^nx$ is divisible by $(x - y)(y - z)(z - x)$.

12. The Euclidean algorithm. Let A_1 and $A_2 \neq 0$ be two polynomials in a field R, and suppose the degree of A_1 to be not less than that of A_2, this supposition being merely a matter of notation. On dividing A_1 by A_2 we obtain a quotient Q_1 and a remainder which is now denoted by A_3. If $A_3 \neq 0$, its degree is less than that of A_2. We may therefore divide A_2 by A_3, obtaining a remainder A_4. If $A_4 \neq 0$, we divide A_3 by A_4; etc. This process (which consists in repeatedly dividing the last divisor employed by the last remainder obtained) must eventually terminate as the degrees of the polynomials A_2, A_3, $\cdots$ are decreasing integers ≥ 0. It

terminates when a zero remainder is obtained. We then have:

$$\begin{aligned}
A_1 &= Q_1A_2 + A_3,\\
A_2 &= Q_2A_3 + A_4,\\
&\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot\\
A_{k-3} &= Q_{k-3}A_{k-2} + A_{k-1},\\
A_{k-2} &= Q_{k-2}A_{k-1} + A_k,\\
A_{k-1} &= Q_{k-1}A_k.
\end{aligned}$$

This method of calculating the A's and Q's is called the *Euclidean algorithm.* All the A's and Q's are polynomials in R.

In assuming, as we did, that the degree of A_1 was not less than that of A_2, the case in which $A_1 = 0$ was excluded. For completeness, the Euclidean algorithm of the polynomials $A_1 = 0$, $A_2 \neq 0$ is defined to consist of the one step:

$$0 = 0 \cdot A_2.$$

13. Greatest common divisor and least common multiple. A polynomial which is a divisor of two or more polynomials is a *common* divisor of these polynomials. A common divisor of two or more polynomials is called their *greatest common divisor* (g.c.d.) if it is divisible by every common divisor of these polynomials. Any associate (see definition, p. 27, Ex. 6) of the g.c.d. of a set of polynomials is also their g.c.d. Two polynomials are *relatively prime* if their g.c.d. is 1.

A polynomial which is a multiple of two or more polynomials is a *common* multiple of these polynomials. A common multiple of two or more polynomials is called their *least common multiple* (l.c.m.) if it is a divisor of every common multiple of these polynomials. Any associate of the l.c.m. of a set of polynomials is also their l.c.m.

THEOREM 2. *The g.c.d. of two polynomials, at least one of which is not* 0, *is the last divisor employed in the Euclidean algorithm of the two polynomials.*

Let A_1 and A_2 be two polynomials, neither of which is the zero-polynomial, and suppose the degree of A_1 to be not less than that of A_2. With the notation of § 12, A_k is the g.c.d. of A_1 and A_2. For the last equation of the Euclidean algorithm of these polynomials asserts that A_k is a divisor of A_{k-1}. From the next to the last equation we infer that, as A_k is a divisor of A_k and of A_{k-1}, A_k is a divisor of A_{k-2}. From the immediately preceding equation we

infer that A_k is a divisor of A_{k-3}; etc. We conclude that A_k is a common divisor of A_1 and A_2.

From the first equation it is evident that, if C is a common divisor of A_1 and A_2, C is a divisor of A_3. From the second equation we infer that, as C is a common divisor of A_2 and A_3, C is a divisor of A_4; etc. We conclude that C is a divisor of A_k.

It follows from the definition of g.c.d. that A_k is the g.c.d. of A_1 and A_2. This is clearly the case if $A_1 = 0$, $A_2 \neq 0$, in which case $A_k = A_2$ (see the last equation of § 12).

EXERCISES

1. Show that if the Euclidean algorithm of two polynomials in a field R is modified by multiplying any of the remainders by an element of R different from 0, the last divisor will still be the g.c.d. of the two polynomials. (This fact is useful in practice.)

2. Show that if D is the g.c.d. of A and B, $(AB \neq 0)$, then A/D and B/D are relatively prime.

3. Show that the g.c.d. of two polynomials A and B in a field R is also the g.c.d. of $A_1 = p_1A + q_1B$ and $B_1 = p_2A + q_2B$, where p_1, p_2, q_1, q_2 are arbitrary elements of R subject to the restriction $p_1q_2 - p_2q_1 \neq 0$. [Express A and B in terms of A_1 and B_1.]

4. Find the g.c.d. of

(a) $x^6 + 3x^5 + 6x^4 + 7x^3 + 6x^2 + 3x + 1$ and
$x^5 + x^4 + x^3 - x^2 - x - 1$. *Ans.* $x^4 + 2x^3 + 3x^2 + 2x + 1$.

(b) $x^6 - 6x^4 + 12x^2 - 8$ and $x^3 - x + 2$. *Ans.* 1.

(c) $x^4 + (2 - 2i)x^3 + (2 - 4i)x^2 + (-1 - 2i)x - 1 - i$ and
$x^2 + (1 - 2i)x + 1 - i$. *Ans.* The second polynomial.

(d) $x^3 + (-4 + \sqrt{3})x - 3 + \sqrt{3}$ and $x^2 - 3$. $x - \sqrt{3}$.

(e) $x^4 - y^2x^3 + (y - 1)x - y^3 + y^2$ and
$x^3 + (-y^2 + y)x^2 + (-y^3 + y^2)x - y^4$. *Ans.* $x - y^2$.

(f) 0 and any other polynomial.

(g) 1 and any polynomial.

5. Determine c so that the g.c.d. of the polynomials

$$x^2 + (c + 6)x + 4c + 2, \qquad x^2 + (c + 2)x + 2c$$

shall be a polynomial of the first degree. *Ans.* $c = 3, 1$.

6. Determine t and u so that the g.c.d. of the polynomials

$$x^3 + (t + 1)x^2 + 2x + 2u, \qquad x^3 + tx^2 + u$$

shall be a polynomial of the second degree.

Ans. t

14. The identity $AG + BF = D$. If D is the g.c.d. of two polynomials A and B in a field R, D is clearly a divisor of every polynomial in the set

$$AV + BU, \tag{1}$$

U and V being arbitrary polynomials in R. The question arises whether D itself is in the set; that is, whether it is possible to find two polynomials F and G in R such that $AG + BF = D$. This question will be answered in the affirmative. It will then follow that every polynomial in R which is a multiple of D is in the set (1).

Referring to the equations of § 12, we have, with the notation $A = A_1$, $B = A_2$, $D = A_k$,

$$D = A_{k-2} - Q_{k-2}A_{k-1} = A_{k-2}V_1 + A_{k-1}U_1,$$

where

$$U_1 = -Q_{k-2}, \qquad V_1 = 1.$$

Since

$$A_{k-1} = A_{k-3} - Q_{k-3}A_{k-2},$$
$$D = A_{k-2}V_1 + (A_{k-3} - Q_{k-3}A_{k-2})U_1 = A_{k-3}V_2 + A_{k-2}U_2,$$

where

$$U_2 = V_1 - Q_{k-3}U_1, \qquad V_2 = U_1.$$

Again, since

$$A_{k-2} = A_{k-4} - Q_{k-4}A_{k-3},$$
$$D = A_{k-3}V_2 + (A_{k-4} - Q_{k-4}A_{k-3})U_2 = A_{k-4}V_3 + A_{k-3}U_3,$$

where

$$U_3 = V_2 - Q_{k-4}U_2, \qquad V_3 = U_2.$$

Continuing thus, we have the

THEOREM 3. *If A and B are two polynomials in a field R and D is their g.c.d., there exist two polynomials U and V in R, such that*

$$AV + BU = D.$$

COROLLARY. *A necessary and sufficient condition that two polynomials A and B be relatively prime is that there exist two polynomials U and V such that*

$$AV + BU = 1.$$

Theorem 3 asserts that the condition is necessary. Conversely, if two polynomials U and V exist such that $AV + BU = 1$, it is obvious that A and B are relatively prime.

The polynomials U and V of Theorem 3 are by no means unique. In fact, if $U = F$ and $V = G$ fulfill the requirements of Theorem 3, so do

$$U = F - TA, \qquad V = G + TB,$$

T being an arbitrary polynomial in R. (This statement may be verified by direct substitution.) U and V may therefore be chosen so as to be of arbitrarily high degree. There are, however, lower limits to their degrees which we proceed to consider. The trivial case $AB = 0$ is excluded.

Dividing the U and the V of Theorem 3 by A and B respectively, the equations

$$U = Q_1A + U_0, \qquad V = Q_2B + V_0$$

are obtained; the remainder in each case, if it does not vanish, having a degree less than that of the divisor. We now have

$$A(Q_2B + V_0) + B(Q_1A + U_0) = D.$$

Therefore

$$D - AV_0 - BU_0 = (Q_1 + Q_2)AB.$$

The degree of the left member of this equation is less than that of AB. Therefore $Q_1 + Q_2 = 0$, and

$$AV_0 + BU_0 = D. \tag{2}$$

One, but not both, of the polynomials U_0 and V_0 may vanish. If $V_0 = 0$, $BU_0 = D$. D is therefore a multiple of B as well as a divisor of B, and U_0 is a constant different from zero. As D is a divisor of A, so is B. Suppose that $A = BC$. Then

$$D = BU_0 = B(U_0 - CG) + GA,$$

G being an arbitrary polynomial. It is obvious that an element $G \neq 0$ of R can be chosen so that $U_0 - CG \neq 0$. The degree of the polynomial $F = U_0 - CG$ is then less than that of A and the degree of G is less than that of B unless A and B are constants.

Combining this result with that embodied in (2), changing the U_0 and V_0 of (2) to F and G respectively, we have the

THEOREM 4. *If A and B are non-constant polynomials in a field R and D is their g.c.d., there exist two polynomials F and G in R whose degrees are less than those of A and B respectively, such that*

$$AG + BF = D.$$

(The reference to the degrees of F and G implies that neither F nor G vanishes.)

We investigate, finally, the uniqueness of these polynomials F and G, beginning with the case in which A and B are non-constant relatively prime polynomials, so that $AG + BF = 1$. Suppose there were another pair of polynomials F_1 and G_1 with degrees less than those of A and B respectively, such that $AG_1 + BF_1 = 1$. Subtracting the two equations, we have

$$A(G - G_1) + B(F - F_1) = 0,$$

from which it follows that A is a divisor of $B(F - F_1)$. Consequently A is a divisor of each term of the left member of the equation

$$(F - F_1)AG + (F - F_1)BF = F - F_1,$$

and therefore also of $F - F_1$. Since the degree of $F - F_1$ is less than the degree of A, $F = F_1$ and $G = G_1$. The polynomials F and G are therefore unique.

Now let A and B be two polynomials in R, neither of which is divisible by the other. If D is their g.c.d., A/D and B/D are non-constant relatively prime polynomials. By the result of the preceding paragraph there exist two unique polynomials F and G whose degrees are less than those of A/D and B/D respectively, such that $(A/D)G + (B/D)F = 1$.

THEOREM 5. *If A and B are two polynomials in a field R, neither of which is divisible by the other, and D is their g.c.d., there exist two unique polynomials F and G in R whose degrees are less than those of A/D and B/D respectively, such that*

$$AG + BF = D.$$

It is found convenient, in practice, to find F and G by the method of undetermined coefficients.

Example. Find polynomials F and G, of lowest possible degree, such that

$$(x^3 - 2x^2 + x - 1)G + (x^2 + x - 3)F = 1.$$

Assuming that the given polynomials are relatively prime, G and F will have the maximum degrees 1 and 2 respectively. Let

$$G = ax + b, \qquad F = cx^2 + dx + e.$$

Then a, b, c, d, e are to be determined so that

$$(x^3 - 2x^2 + x - 1)(ax + b) + (x^2 + x - 3)(cx^2 + dx + e) = 1.$$

Expanding, we must have

$$\begin{aligned} a + c &= 0, \\ -2a + b + c + d &= 0, \\ a - 2b - 3c + d + e &= 0, \\ -a + b - 3d + e &= 0, \\ -b - 3e &= 1. \end{aligned}$$

Solving this system of linear equations, we obtain

$$a = -7/23,\ b = -17/23,\ c = 7/23,\ d = -4/23,\ e = -2/23.$$

Hence

$$G = \tfrac{1}{23}(-7x - 17), \qquad F = \tfrac{1}{23}(7x^2 - 4x - 2).$$

Had our assumption that the given polynomials are relatively prime been false, some absurdity (such as $1 = 0$) would have appeared in the course of the calculations.

EXERCISES

1. Find polynomials F and G, of lowest possible degree, such that

(a) $(x^3 - 3x + 1)G + (x^2 + x + 1)F = 1.$

Ans. $G = \frac{1}{19}(3x + 5), \qquad F = \frac{1}{19}(-3x^2 - 2x + 14).$

(b) $(x^3 - x^2 + 2x - 4)G + (x + 3)F = 1.$

Ans. $G = -\frac{1}{46}, \qquad F = \frac{1}{46}(x^2 - 4x + 14).$

(c) $(x^4 - x - 1 + i)G + (x^2 + 1)F = x - i.$

Ans. $G = -1, \qquad F = x^2 - 1.$

(d) $[x^2 + (y - 1)x + 1]G + [x^2 + (y + 1)x + 2]F = 1.$

Ans. $G = -\dfrac{2x + 2y + 1}{2y - 7}, \qquad F = \dfrac{2x + 2y - 3}{2y - 7}.$

2. In trying to find F and G such that

$$(x^2 + x - 2)G + (x^2 - x)F = 1,$$

an absurdity is obtained. Why?

3. Prove that every common root of two polynomials is a root of their g.c.d., and conversely.

4. Solve the equation $2x^4 + 9x^2 + 17x - 21 = 0$, which has a root in common with the equation $x^3 + 2x^2 + 4x + 21 = 0$.

5. Solve the equation $x^4 - 4x^3 + 6x^2 - 7x + 2 = 0$, which has two roots whose product is 1. *Ans.* $\dfrac{3 \pm \sqrt{5}}{2}, \dfrac{1 \pm \sqrt{-7}}{2}$.

[Denoting the left member by $f(x)$, observe that $f(x) = 0$ and $x^4f(1/x) = 0$ have a root in common.]

6. The equation $x^6 + x^5 + x^4 - x^3 - 14x^2 - 6x + 6 = 0$ has two roots whose sum is 0. Find them. *Ans.* $\pm\sqrt{3}$.

7. Determine k so that the difference of two of the roots of the equation $x^3 - 28x + k = 0$ shall be 2, and find the roots.

Ans. $k = 48$, roots $2, 4, -6$; $k = -48$, roots $-2, -4, 6$.

8. Show that if $A(x)$ and $B(x)$ are relatively prime polynomials, then $A(x^m)$ and $B(x^m)$ are relatively prime polynomials. Generalize. [Use the corollary to Theorem 3.]

15. Subfields. Reducibility. If every element of a field R_1 is an element of a field R_2, R_1 is a *subfield* of R_2 and R_2 is a *superfield* of R_1. In particular, every field is a subfield as well as a superfield of itself.

Example 1. Every number-field is a subfield of the field of complex numbers.

Example 2. The field generated by a primitive nth root of unity is a superfield of the field generated by a primitive dth root of unity if d is a divisor of n.

Example 3. If R_1 is a subfield of R_2, $R_1(x)$ is a subfield of $R_2(x)$.

A polynomial in a field R is *reducible* in R if it equals the product of two polynomials in R, neither of which is a constant. In the contrary case, the polynomial is *irreducible* in R. The equation $A(x) = 0$ is *reducible* or *irreducible* in R according as the polynomial $A(x)$ is reducible or irreducible in R.

Example 4. The polynomial $ax + b$, where a and b are elements of a field R, is irreducible in R.

Example 5. The polynomial $x^2 + 1$ is reducible in a number-field R which contains i and is irreducible otherwise.

For, suppose that

$$x^2 + 1 = (ax + b)(cx + d),$$

where a, b, c, and d are elements of R. Expanding the right member and equating coefficients of like powers of x, we have

$$ac = 1,$$
$$ad + bc = 0,$$
$$bd = 1.$$

Solving the first and third of these equations for c and d respectively and substituting in the second, we have $a^2 + b^2 = 0$, so that $a/b = \pm i$. Therefore R contains the number i. Conversely, if R contains i, $x^2 + 1$ is reducible in R; for $x^2 + 1 = (x + i)\cdot(x - i)$.

Example 6. The polynomial $x^3 - 1$ is reducible in $R(1)$ and therefore in every field; for

$$x^3 - 1 = (x - 1)(x^2 + x + 1).$$

The polynomial is *further* reducible in every field containing $\sqrt{-3}$; for

$$x^3 - 1 = (x - 1)\left(x - \frac{-1 + \sqrt{-3}}{2}\right)\left(x - \frac{-1 - \sqrt{-3}}{2}\right).$$

It is to be emphasized that the concept of reducibility of a polynomial (or equation) has a meaning only with reference to a specified field which contains the coefficients of the polynomial (or equation). A polynomial may be reducible in one field but irreducible in another.

THEOREM 6. *If the product of two polynomials A and B is divisible by a polynomial C which is prime to B, then A is divisible by C.*

As B and C are relatively prime, there exist two polynomials F and G, such that

$$BG + CF = 1.$$

Multiplying each term by A, we have

$$ABG + ACF = A.$$

By hypothesis, $AB = QC$, where Q is a polynomial. Therefore

$$C(QG + AF) = A,$$

which asserts that A is divisible by C.

THEOREM 7. *If the product of two polynomials A and B in a field R is divisible by a polynomial P which is irreducible in R, at least one of the polynomials A and B must be divisible by P.*

The only divisors in R of P are associates of P and constants.

Therefore, if A is not divisible by P, A is prime to P. It follows from Theorem 6 that B is divisible by P.

16. Unique Factorization Theorem. A *primary* polynomial is one whose leading coefficient is 1. Every polynomial $\neq 0$ is expressible as the product of its leading coefficient and a primary polynomial:

$$a_0x^n + a_1x^{n-1} + \qquad + a_{n-1}x + a_n = a_0\left(x^n + \frac{a_1}{a_0}x^{n-1} + \cdots + \frac{a_{n-1}}{a_0}x + \frac{a_n}{a_0}\right).$$

More briefly:

$$A(x) = a_0A_1(x), \tag{1}$$

where a_0 is the leading coefficient of the polynomial $A(x)$, and $A_1(x)$ is a primary polynomial.

If $A_1 = A_1(x)$ is reducible in a field R containing the coefficients of $A = A(x)$, A_1 may clearly be expressed as the product of two *primary* polynomials in R. Treating each of these factors in the same way, we finally obtain

$$A = a_0P_1P_2 \cdots P_s, \tag{2}$$

where $P_1, P_2, \cdots, P_s$ are primary *irreducible* polynomials in R, and s is some positive integer.

Suppose we also had

$$A = a_0'Q_1Q_2 \cdots Q_t, \tag{3}$$

where a_0' is an element of R, and $Q_1, Q_2, \cdots, Q_t$ are primary irreducible polynomials in R. Then $a_0 = a_0'$, each being the leading coefficient of A. Therefore

$$P_1P_2 \qquad P_s = Q_1Q_2 \qquad Q_t. \tag{4}$$

By Theorem 7, Q_1 is a divisor of at least one of the P's, say P_1. Therefore $P_1 = Q_1U$, U being a polynomial in R. Since P_1 is irreducible in R, U is a constant; and, since P_1 and Q_1 are primary polynomials, $U = 1$. Therefore $P_1 = Q_1$. From (**4**) we have

$$P_s = Q_2 \qquad Q_t.$$

Applying the same argument to this equation, we finally arrive at the conclusion that each of the Q's equals one of the P's, and that $s = t$. Therefore the right members of (**2**) and (**3**) are identical

except, perhaps, as regards the order in which the factors are written. This result is known as the *Unique Factorization Theorem.*

THEOREM 8. *Every polynomial in a field R can be expressed as the product of its leading coefficient and one or more primary irreducible polynomials in R in one, and in only one way, except for the order in which the factors may be written.*

Returning to (2), it may happen that some of the P's are equal. Collecting those which are equal, we write

$$(5) \qquad A = a_0 P_1^{n_1} P_2^{n_2} \qquad P_r^{n_r}, \qquad (n_i \geq 1;\ i = 1, \qquad , r),$$

where $P_1, P_2, \cdots, P_r$ are *distinct* primary irreducible polynomials in R, and $r \leq s$. (5) is called the *canonical form* of A. If A is irreducible in R, its canonical form is (1). We therefore have, as an alternative form of the Unique Factorization Theorem, the

THEOREM 9. *Every polynomial in a field R may be expressed in the canonical form* (5) *in one, and in only one way, except for the order in which the factors may be written.*

The canonical form of a polynomial may be different for different fields.

Example. The canonical form of the polynomial $x^2 + 1$ is $x^2 + 1$ if the field does not contain i, but is $(x + i)(x - i)$ if the field does contain i. (See Example 5 of § 15).

EXERCISES

1. Show that the field of rational numbers has no subfield besides itself. (Because of this property the field of rational numbers is called a *prime* field.)

2. Find the subfields of

(a) $R(\sqrt{2})$. (b) $R(\sqrt[3]{2})$. (c) $R(\sqrt[4]{2})$.

3. (a) Find the roots of the equation $x^4 + 1 = 0$ (§ 7), and express $x^4 + 1$ as the product of four linear polynomials in $R\left(\dfrac{\sqrt{2} + i\sqrt{2}}{2}\right)$.

(b) Show that $x^4 + 1$ equals the product of two irreducible quadratic polynomials in each of the fields $R(i)$, $R(\sqrt{2})$, $R(i\sqrt{2})$.

(c) Show that $x^4 + 1$ is irreducible in $R(1)$.

(d) Show that $x^4 + 1$ is irreducible in a field which contains none of the numbers i, $\sqrt{2}$, $i\sqrt{2}$; that it equals the product of two irreducible quadratic polynomials in a field which contains one and only one of these numbers; and that it equals the product of four linear polynomials in a field which contains all three of these numbers.

(e) Where is the Unique Factorization Theorem invoked in arriving at the preceding results?

4. Treat similarly each of the polynomials

(a) $x^4 - 10x^2 + 1$. (c) $x^3 - 2$.
(b) $x^4 - 14x^2 + 9$. (d) $x^4 + x^2 + 1$.

5. Show that every complex number satisfies either a linear or a quadratic equation with real coefficients which is irreducible in the field of real numbers.

6. Show that every element of $R(\sqrt{2})$ satisfies either a linear or a quadratic equation with rational coefficients which is irreducible in $R(1)$. Generalize.

7. Show that a polynomial which is prime to each of two polynomials is prime to their product.

8. Show that a polynomial which is divisible by each of two relatively prime polynomials is divisible by their product.

9. Show that, if ϵ is a primitive nth root of unity,

$$x^n - 1 = (x - 1)(x - \epsilon)(x - \epsilon^2) \cdots (x - \epsilon^{n-1}).$$

10. Show that if $A/B = C/D$, where A, B, C, and D are polynomials, and C and D are relatively prime, then A is divisible by C, and B by D.

11. Show that *all* pairs of polynomials f and g in a field R which satisfy the equation $Ag + Bf = 1$, where A and B are relatively prime polynomials in R, are included in the system

$$f = F - TA, \qquad g = G + TB,$$

where T is an arbitrary polynomial in R, and F and G are fixed polynomials in R which satisfy $AG + BF = 1$.

12. Show that if (5) is the canonical form of a polynomial A in a field R, every divisor of A in R has the form

$$a'P_1^{p_1}P_2^{p_2} \cdots P_r^{p_r}, \qquad (0 \leq p_i \leq n_i;\ i = 1, \cdots, r).$$

13. If each of two polynomials is expressed in the canonical form, how may their g.c.d. be determined?

14. Show that the l.c.m. of two relatively prime polynomials equals their product.

15. Show that the l.c.m. of two polynomials equals their product divided by their g.c.d.

16. How may the l.c.m. of a set of polynomials in a field R be determined when each of the polynomials is expressed in its canonical form?

17. Find an equation satisfied by $\sqrt[3]{2} + \sqrt{2}$

(a) in $R(\sqrt[3]{2})$. (b) in $R(\sqrt{2})$. (c) in $R(1)$.

Ans. (c) $x^6 - 6x^4 - 4x^3 + 12x^2 - 24x - 4 = 0$.

18. Find the irreducible equation in $R(1)$ which is satisfied by $\sqrt[3]{2} + \sqrt[3]{4}$. [See Example 5, p. 20.] *Ans.* $x^3 - 6x - 6 = 0$.

19. Show that if n is divisible by d, $x^n - 1$ is divisible by $x^d - 1$.

20. Conversely, if $x^n - 1$ is divisible by $x^d - 1$, n is divisible by d. [Use the result of Ex. 8, p. 16.]

21. Show that if d is the g.c.d. of m and n, $x^d - 1$ is the g.c.d. of $x^m - 1$ and $x^n - 1$.

22. Find the equation whose roots are the primitive 15th roots of unity. [See Ex. 5, p. 16.] *Ans.* $x^8 - x^7 + x^5 - x^4 + x^3 - x + 1 = 0$.

23. Let $F_m(x)$ denote the primary polynomial whose roots are the primitive mth roots of unity; for example,

$$F_1(x) = x - 1, \quad F_2(x) = x + 1, \quad F_3(x) = x^2 + x + 1, \quad F_4(x) = x^2 + 1.$$

Verify that

(a) $x^4 - 1 = F_1(x)F_2(x)F_4(x)$.
(b) $x^8 - 1 = F_1(x)F_2(x)F_4(x)F_8(x)$.
(c) $x^6 - 1 = F_1(x)F_2(x)F_3(x)F_6(x)$.
(d) $x^9 - 1 = F_1(x)F_3(x)F_9(x)$.

24. Let $d_1, d_2, \cdots, d_r$ be the distinct positive divisors of n, including 1 and n. Prove that (as suggested by the preceding exercise)

$$x^n - 1 = F_{d_1}(x)F_{d_2}(x) \qquad F_{d_r}(x).$$

[See Ex. 10, p. 16.]

25. Show that the primitive nth roots of unity satisfy an equation with *integral* coefficients.* [Prove first for n = a prime number; then apply mathematical induction, using the result of Ex. 24.]

* It is somewhat more difficult to prove that this equation is *irreducible* in $R(1)$. Assuming that this is the case, the result of Ex. 24 gives a complete factorization of $x^n - 1$ in $R(1)$. See § 69.

CHAPTER III

FURTHER PROPERTIES OF POLYNOMIALS IN A FIELD

17. Polynomials and equations having assigned roots. If at least one of the irreducible factors of a polynomial $A(x)$ in a field R is linear, the canonical form of $A(x)$ for the field R assumes the form

$$(1)\quad A(x) = a_0(x - x_1)^{m_1} \cdots (x - x_k)^{m_k}[P_1(x)]^{n_1} \cdots [P_t(x)]^{n_t},$$
$$(k \geq 1; t \geq 0; m_i \geq 1, i = 1, \cdots, k; n_i \geq 1, i = 1, \cdots, t),$$

where $x_1, \cdots, x_k$ are distinct elements of R and (in the event that $t \geq 1$) $P_1(x), \cdots, P_t(x)$ are irreducible polynomials in R of degree ≥ 2. Since

$$A(x_i) = 0, \qquad (i = 1, \cdots, k),$$

x_i is a root of the polynomial $A(x)$ and of the equation $A(x) = 0$. Moreover, no element of R besides $x_1, \cdots, x_k$ is a root of $A(x)$. For, if r is a root in R of $A(x)$, $x - r$ is a factor of $A(x)$, (Factor Theorem, p. 27, Ex. 10), and must, by the Unique Factorization Theorem, be one of the polynomials $x - x_1, \cdots, x - x_k$, as $x - r$ cannot be a factor of any of the polynomials $P_1(x), \cdots, P_t(x)$.

For the same reason $A(x)$ cannot be divisible by $(x - x_i)^{m_i+1}$. x_i is therefore called an m_i-fold root of $A(x)$, or a root of *multiplicity* m_i. If $m_i = 1$, x_i is a *simple* root; if $m_i \geq 2$, x_i is a *repeated* or *multiple* root. If $m_i = 2$, x_i is a *double* root; if $m_i = 3$, x_i is a *triple* root; etc.

It is more convenient for certain purposes to write (1) in the form

$$(2)\qquad A(x) = (x - x_1) \cdots (x - x_s)B(x),$$

where $x_1, \cdots, x_s$ are the roots in R of $A(x)$, not necessarily distinct, while $B(x)$ is a polynomial in R which has no root in R. To an m-fold root of $A(x)$ there correspond exactly m equal linear factors in the right member of (2). Unless the contrary is explicitly

stated or implied by the context, the roots of a polynomial are not to be assumed distinct. When we state that $x_1, \cdots, x_h$ are roots in R of $A(x)$, we do not imply that these are the only roots in R of $A(x)$. If, however, among the roots $x_1, \cdots, x_h$, a certain root is repeated l times, it is to be understood that this root is *at least* an l-fold root of $A(x)$. With these agreements we have, as an immediate consequence of (**2**), the

THEOREM 1. *A polynomial $A(x)$ in a field R, of which $x_1, \cdots, x_h$ are roots in R, is divisible by the polynomial*

$$(x - x_1) \cdots (x - x_h).$$

If the degree of $A(x)$ is n and, in (**2**), $s = n$, $B(x)$ must be a constant which is clearly the leading coefficient of $A(x)$.

THEOREM 2. *A polynomial $A(x)$ of degree n in a field R, which has n roots $x_1, \cdots, x_n$ in R, can be represented uniquely in the form*

$$A(x) = a_0(x - x_1) \cdots (x - x_n),$$

where a_0 is the leading coefficient of $A(x)$. Conversely, if $A(x)$ is representable in this form it has the roots $x_1, \cdots, x_n$, and no additional roots.

EXERCISES

1. Construct an equation whose roots are

(a) $0, 2, \frac{1}{2}$.

(b) $3, 1 + \sqrt{5}, 1 - \sqrt{5}$.

(c) $2 + 3i, 2 - 3i, 2 + \sqrt{2}, 2 - \sqrt{2}$.

(d) $\frac{1 + i\sqrt{3}}{2}, \frac{1 - i\sqrt{3}}{2}, i, -i$.

(e) $2 + i, \sqrt{3}, 1$.

(f) $1, 1, 1, -1$.

(g) $0, 0, -1 + i, -1 + i$.

(h) $t + 1, t + i, t - i, 0$.

2. Find the roots, in the field of complex numbers, of

(a) $x^2(x^2 - 8x + 12) = 0$.

(b) $(x^2 + x - 1)(x^2 - x + 1) = 0$.

(c) $(x^2 - 4)^3 = 0$.

(d) $(x^2 + 2x + 2)^2(x^2 - 1)^2 = 0$.

3. Can an algebraic equation with at least one irrational coefficient have a rational root?

4. Can an algebraic equation with at least one imaginary coefficient have a real root?

5. Determine a so that -2 shall be a root of the equation

$$x^3 + 2ax^2 + (a + 1)x - 3 = 0.$$

6. Determine a and b so that 1 shall be a double root of the equation

$$x^4 + ax^3 + (a - b)x^2 + bx + 1 = 0.$$

7. Show that an equation of degree n in a field R has at most n roots in R.

8. Show that it is impossible to find three distinct numbers, the square of each of which equals the sum of the other two. [Show that the three numbers would satisfy the equation $x^2 + x - s = 0$, where s denotes their sum.]

9. Show that it is impossible to find four distinct numbers, the square of each of which equals the product of the other three.

10. Show that two polynomials of degree $\leq n$ in a single variable are equal (see definition, p. 24) if they assume the same values for $n + 1$ distinct values of the variable.

11. Show that the trigonometric functions $\sin x$, $\cos x$, etc. are not polynomials. Show that they are not rational functions.

12. Show that if r is an a-fold root of $A(x)$ and a b-fold root of $B(x)$, then r is an $(a + b)$-fold root of $A(x)B(x)$.

13. (a) Show that if ϵ is a primitive nth root of unity,

$$x^{n-1} + x^{n-2} + \cdots + x + 1 = (x - \epsilon)(x - \epsilon^2) \cdots (x - \epsilon^{n-1}), \quad (n \geq 2).$$

(b) Deduce that

$$n = (1 - \epsilon)(1 - \epsilon^2) \cdots (1 - \epsilon^{n-1}), \quad (n \geq 2).$$

(c) Using the result of Ex. 13, p. 14, show that

$$\sin \frac{\pi}{n} \sin \frac{2\pi}{n} \cdots \sin \frac{(n-1)\pi}{n} = \frac{n}{2^{n-1}}, \quad (n \geq 2).$$

18. Relations between roots and coefficients. If the polynomial

$$A(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n, \quad (a_0 \neq 0)$$

in a field R has n roots $x_1, \cdots, x_n$ in R,

$$A(x) = a_0(x - x_1)(x - x_2) \cdots (x - x_n).$$

Equating coefficients of like powers of x of the identity in x

$$a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n = a_0(x - x_1)(x - x_2) \cdots (x - x_n),$$

we obtain

$$\Sigma x_1 = x_1 + x_2 + \cdots + x_n = -\frac{a_1}{a_0},$$

$$\Sigma x_1x_2 = x_1x_2 + x_1x_3 + x_2x_3 + \cdots + x_{n-1}x_n = +\frac{a_2}{a_0},$$

$$\Sigma x_1x_2x_3 = x_1x_2x_3 + x_1x_2x_4 + \cdots + x_{n-2}x_{n-1}x_n = -\frac{a_3}{a_0},$$

$$\Sigma x_1x_2 \cdots x_n = x_1x_2 \cdots x_n = (-1)^n \frac{a_n}{a_0}.$$

The first member of each of these equations is an abbreviation for the expression written more fully in the second member. The rth equation asserts that the *sum of all the possible products of the roots taken r at a time equals* $(-1)^r a_r/a_0$.

The relations between the roots and coefficients of an equation are useful in constructing an equation whose roots have an assigned relation to the roots of a given equation, and in solving an equation when some relation among the roots is given.

Example 1. Find the equation whose roots are the squares of the roots of the equation $ax^2 + bx + c = 0$.

First solution: Let x_1 and x_2 be the roots of the given equation; then $y_1 = x_1^2$ and $y_2 = x_2^2$ are the roots of the required equation. Now

$$y_1 + y_2 = x_1^2 + x_2^2 = (x_1 + x_2)^2 - 2x_1x_2 = \frac{b^2}{a^2} - \frac{2c}{a} = \frac{b^2 - 2ac}{a^2},$$

$$y_1y_2 \quad x_1^2x_2^2 = \frac{c^2}{a^2}.$$

The required equation is therefore

$$a^2y^2 + (2ac - b^2)y + c^2 = 0.$$

Second solution: Substitute $x = \sqrt{y}$ in the given equation, obtaining

$$ay + b\sqrt{y} + c = 0,$$

whence

$$(ay + c)^2 = b^2y.$$

Simplifying, we obtain the required equation

$$a^2y^2 + (2ac - b^2)y + c^2 = 0.$$

Note: The second method is usually simpler when each root of the required equation is the same function of *one* of the roots of the given equation. The first method is more general and can be used in a wider variety of problems than the second.

Example 2. Determine k so that one root of the equation

$$x^3 - 13x^2 - 65x + k = 0$$

shall be three times another; and find the roots.

Denoting the roots by x_1, x_2, x_3, we take $x_2 = 3x_1$. Substituting

in the first two of the relations between the roots and coefficients:

$$\begin{aligned} x_1 + x_2 + x_3 &= 13, \\ x_1x_2 + x_1x_3 + x_2x_3 &= -65, \\ x_1x_2x_3 &= -k, \end{aligned}$$

we obtain

$$\begin{aligned} 4x_1 + x_3 &= 13, \\ 3x_1^2 + 4x_1x_3 &= -65. \end{aligned}$$

Eliminating x_3, we obtain

$$x_1^2 - 4x_1 - 5 = 0,$$

from which it follows that $x_1 = -1$, $x_1 = 5$. There are therefore *two* answers:

$x_1 = -1, x_2 = 3x_1 = -3, x_3 = 13 - 4x_1 = 17, k = -x_1x_2x_3 = 51;$
$x_1 = 5, x_2 = 15, x_3 = -7, k = 525.$

EXERCISES

1. Write in full the relations between the roots and coefficients of a quartic equation.

2. How many terms does $\Sigma x_1x_2 \cdots x_r$ involve?

3. Find the equation whose roots are the squares of the roots of the equation $x^3 - \sqrt{3}x + 1 = 0$.

4. Find the equation whose roots are the cubes of the roots of the equation $x^2 - 2ix + 1 - i = 0$. *Ans.* $y^2 + (6 + 14i)y - 2 - 2i = 0$.

5. Find the equation whose roots are twice the roots of the equation $x^4 + x^3 - 7x^2 + 8x - 2 = 0$.

6. Find the equation whose roots are 3 less than the roots of the equation $x^3 - 9x^2 + 4x - 4 = 0$.

7. Find the equation whose roots are the reciprocals of the roots of the equation $x^5 - 3x^3 + 9x^2 - 8x + 11 = 0$.

8. Show that the reciprocal of each root of the equation

$$ax^4 + bx^3 + cx^2 + bx + a = 0 \qquad (a \neq 0)$$

is also a root.

9. Denoting the roots of the equation $x^3 - 3x + 1 = 0$ by x_1, x_2, x_3, find the equation whose roots are

$$\frac{3x_1 + 2}{x_1 + 1}, \quad \frac{3x_2 + 2}{x_2 + 1}, \quad \frac{3x_3 + 2}{x_3 + 1}.$$

Ans. $3y^3 - 27y^2 + 78y - 73 = 0$.

10. Determine k so that one root of the equation $x^3 - 7x + k = 0$ shall be twice another; and find the roots.

11. Determine k so that the sum of two roots of the equation

$$x^3 + 5x^2 + kx - 10 = 0$$

shall be 0; and find the roots.

12. Determine k so that the equation

$$3x^3 + 11x^2 + 8x + k = 0$$

shall have two equal roots; and find the roots.

13. Determine a, b, and c so that all the roots of the equation

$$x^4 + ax^3 + 24x^2 + bx + c = 0$$

shall be equal; and find the roots.

14. Determine k so that the product of two of the roots of the equation

$$x^3 + kx^2 - kx + 2 = 0$$

shall be 1; and find the roots.

15. Solve Ex. 7, p. 34, using the relations between the roots and coefficients.

16. The lengths of the sides of a triangle are the roots of the equation

$$ax^3 + bx^2 + cx + d = 0.$$

Find the area. [Recall that the area of a triangle whose sides are x_1, x_2, x_3, is $\sqrt{s(s - x_1)(s - x_2)(s - x_3)}$, where s denotes one-half the perimeter.]

Ans. $\dfrac{1}{4a^2}\sqrt{-b^4 + 4ab^2c - 8a^2bd}.$

17. The vertices of a triangle in the z-plane are the roots of the equation

$$az^3 + bz^2 + cz + d = 0.$$

Find the equation whose roots are the midpoints of the sides. [See p. 6, Ex. 12.]

18. Find the condition that the points z_1, z_2, z_3 be the vertices of an equilateral triangle. [See p. 19, Ex. 11.]

19.* Show that the equation

$$a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n = 0 \qquad (a_0 \neq 0)$$

in the field of complex numbers, has at least one root whose absolute value is $\leq$, and at least one root whose absolute value is $\geq$ $\dfrac{a_n}{a_0}$

20.* Show that if the absolute value of every root of the equation of Ex. 19 is $\leq M$, then

$$\frac{a_1}{a_0} \leq nM, \quad \left|\frac{a_2}{a_0}\right| \leq \frac{n(n-1)}{2!}M^2, \qquad \leq \frac{n(n-1)(n-2)}{3!}M^3, \cdots,$$

$$\frac{a_n}{a_0} \leq M^n.$$

21.* Show that it is possible to choose t so large that the absolute value

* In Exercises 19, 20, and 21, assume that an equation of degree n in the field of complex numbers has exactly n roots (not necessarily distinct) in that

of at least one root of the equation

$$x^4 + 3tx^3 - 5x^2 + (t^3 + 1)x - 2 = 0$$

is greater than any preassigned number. Generalize.

19. Derivative of a polynomial in an arbitrary field. The derivative of a function is defined in the Calculus with the aid of the notions of continuity and limit. As there are many fields in which these concepts are meaningless, a different definition is desirable, at least of the derivative of a polynomial. We may, if we wish, simply define the derivative of the polynomial

$$A(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$$

in a field R to be

$$A'(x) = na_0x^{n-1} + (n-1)a_1x^{n-2} + \cdots + 2a_{n-2}x + a_{n-1},$$

and then establish the standard rules of differentiation from this definition. The following method seems less artificial.

The polynomial

$$A(y) - A(x) = a_0(y^n - x^n) + a_1(y^{n-1} - x^{n-1}) + \cdots + a_{n-1}(y - x)$$

is divisible by $y - x$, y being a new variable; in fact,

$$\begin{aligned}\frac{A(y) - A(x)}{y - x} = {} & a_0(y^{n-1}x + y^{n-2}x^2 + \cdots + y^2x^{n-2} + yx^{n-1}) \\ & + a_1(y^{n-2}x + y^{n-3}x^2 + \cdots + y^2x^{n-3} + yx^{n-2}) \\ & + \cdots \\ & + a_{n-2}(y + x) + a_{n-1}.\end{aligned}$$

The left member is undefined for $y = x$ since it then assumes the indeterminate form 0/0. On the other hand the right member has a perfectly definite value for $y = x$. We therefore use the preceding equation to *define* the value of the left member for $y = x$, and write

$$\left.\frac{A(y) - A(x)}{y - x}\right]_{y=x} = na_0x^{n-1} + (n-1)a_1x^{n-2} + \quad + 2a_{n-2}x + a_{n-1}.$$

Observing that the right member of this equation is $A'(x)$, the

field. This theorem follows from the Fundamental Theorem of Algebra, a proof of which will be given subsequently.

derivative of a polynomial $A(x)$ in a field R is now *defined* by

$$\frac{dA}{dx} = A'(x) \quad \left.\frac{A(y) - A(x)}{y - x}\right]_{y=x}$$

It will be noticed that the concepts of continuity and limit are avoided in this definition. The derivative of a rational function in an arbitrary field may be defined similarly. But the derivative of a transcendental function, such as e^x or $\sin x$, cannot be defined in this way. In fact, there are fields in which these functions are undefined.

The standard rules of differentiation are readily established with the aid of the preceding definition of derivative. For example, the rule for the derivative of the product of two polynomials is an immediate consequence of the identity

$$A(y)B(y) - A(x)B(x) = A(y)[B(y) - B(x)] + B(x)[A(y) - A(x)].$$

20. Repeated factors of a polynomial. If a polynomial $A(x)$ is divisible by $[B(x)]^m$, $(m \geq 0)$, but not by $[B(x)]^{m+1}$, $B(x)$ is called an m-fold factor of $A(x)$, or a factor of *multiplicity* m. If $m \geq 2$, $B(x)$ is a *repeated* or *multiple* factor of $A(x)$. A factor of multiplicity 1 is a *simple* factor, a factor of multiplicity 2 a *double* factor, etc. These definitions are obvious extensions of those of § 17.

Let B be an m-fold factor of A, $(m \geq 1)$, so that

$$A = B^mC,$$

C being a polynomial which is not divisible by B. Differentiating, we have

$$A' = B^mC' + mB^{m-1}B'C = B^{m-1}(BC' + mB'C).$$

A' is therefore divisible by B^{m-1}, so that B is *at least* an $(m - 1)$-fold factor of A'. If B and B' are relatively prime, A' cannot be divisible by B^m. For, in that case, $BC' + mB'C$, and therefore $B'C$, would be divisible by B, as $m \neq 0$. Hence, since B and B' are relatively prime, C would be divisible by B, contrary to assumption.

THEOREM 3. *If B is an m-fold factor of A, $(m \geq 1)$, B is at least an $(m - 1)$-fold factor of A'. If, further, B and B' are relatively prime, B is precisely an $(m - 1)$-fold factor of A'.*

It is to be emphasized that, in any case, *every repeated factor of a polynomial A is a factor of A' and therefore of the g.c.d. of A and A'.*

Corollary 1. *A polynomial has no repeated factor if, and only if, it is prime to its derivative.*

Corollary 2. *A polynomial in a field R which has no repeated factor in R has no repeated factor in a superfield of R.*

Corollary 3. *A polynomial which is irreducible in a field R has no repeated factor in R nor in any superfield of R.*

Some of the exponents which occur in the canonical form

$$(1) \qquad A \quad a_0P_1^{n_1}P_2^{n_2} \qquad P_r^{n}$$

of a polynomial A in a field R may be equal. Collecting those P's which have the same exponent, we obtain

$$(2) \qquad A = a_0B_1^{m_1}B_2^{m_2} \cdots B_s^{m_s}, \qquad (1 \leq s \leq r),$$

where a_0 *is the leading coefficient of* A; $m_1, m_2, \cdots, m_s$ *are distinct positive integers; each* B *is the product of distinct irreducible primary polynomials in* R *of degree* ≥ 1 (*and is therefore prime to its derivative*); *and no two of the* B*'s have a factor in common besides constants.* This representation of A is clearly unique, except for the order in which the factors may be written. It will be referred to as the *secondary* canonical form of the polynomial A.

With the aid of the preceding results we shall derive a method of expressing a polynomial in its secondary canonical form by purely rational processes. As each B in (2) is prime to its derivative, the following theorem is a consequence of Theorem 3.

Theorem 4. *If* (2) *is the secondary canonical form of the polynomial* A, *the g.c.d. of* A *and* A' *is*

$$B_1^{m_1-1}B_2^{m_2-1} \qquad B_s^{m_s-1}$$

Corollary. *If* A_1 *is the g.c.d. of* A *and* A', *and* m_1 *is the smallest of the integers* $m_1, m_2, \cdots, m_s$ *which occur in* (2), *the secondary canonical form of* A_1 *is either*

$$(3) \qquad A_1 = a_1B_1^{m_1-1}B_2^{m_2-1} \qquad B_s^{m_s-1} \qquad (a_1 \neq 0)$$

or

$$(4) \qquad A_1 = a_1B_2^{m_2-1} \cdot \qquad B_s^{m} \qquad (a_1 \neq 0)$$

according as $m_1 > 1$ *or* $m_1 = 1$.

Now suppose that A_1, the g.c.d. of A and A', has been calculated and expressed in its secondary canonical form

$$(5) \qquad A_1 = a_1C_1^{q_1}C_2^{q_2} \cdots C_h^{q_h},$$

which must be identical with (3) or (4), except for the order in which the factors are written. In either case A is divisible by

$$C = C_1^{q_1+1}C_2^{q_2+1} \ . \ . \ . \ C_h^{q_h+1},$$

which equals either

$$B_1^{m_1}B_2^{m_2} \qquad B_s^{m_s}$$

or

$$B_2^{m} \qquad B_s^{m}$$

according as $m_1 > 1$ or $m_1 = 1$. If $m_1 > 1$, C and A have the same degree, and A is immediately expressible in its secondary canonical form (2), since $A = a_0C$. If $m_1 = 1$, C is of lower degree than A and is not divisible by B_1. In this case B_1 is found by dividing A by C, and A is then readily written in its secondary canonical form, since $A = a_0B_1C$.

The problem of expressing A in its secondary canonical form therefore reduces to that of expressing A_1 in its secondary canonical form, which, in turn, reduces to that of expressing the g.c.d. of A_1 and A_1' in its secondary canonical form; etc. Hence, every polynomial can be expressed in its secondary canonical form by means of a finite number of rational operations. Moreover, the preceding theory furnishes a practical method of effecting these calculations, as illustrated in the following example.

Example. Express the polynomial

$$A(x) = x^8 - 10x^6 - 8x^5 + 15x^4 + 8x^3 - 10x^2 + 1$$

in its secondary canonical form.

The derivative of $A(x)$ is

$$A'(x) = 8x^7 - 60x^5 - 40x^4 + 60x^3 + 24x^2 - 20x.$$

As x is a factor of $A'(x)$ but not of $A(x)$, the g.c.d. of $A(x)$ and $A'(x)$ is the g.c.d. of $A(x)$ and

$$2x^6 - 15x^4 \qquad 10x^3 + 15x^2 + 6x - 5,$$

which is found to be

$$A_1 = x^4 + 2x^3 - x^2 - 2x + 1.$$

The g.c.d. of A_1 and A_1' is

$$A_2 = x^2 + x - 1,$$

which is prime to its derivative. The process of differentiating, etc. stops at this point as the secondary canonical form of A_2 is A_2.

By the theory, A_1 is divisible by A_2^2. Now A_1 and A_2^2 are primary polynomials of the same degree. Therefore

$$A_1 = A_2^2 = (x^2 + x - 1)^2$$

Again, according to the theory, A is divisible by $(x^2 + x - 1)^3$, which is of lower degree than A. Therefore one of the factors which occurs in the secondary canonical form of A appears to the first power only. Dividing, we find this factor to be $x^2 - 3x - 1$. The secondary canonical form of $A(x)$ is therefore

$$A(x) = (x^2 + x - 1)^3(x^2 - 3x - 1).$$

EXERCISES

1. Express each of the following polynomials in its secondary canonical form.

(a) $x^3 + (1 - i)x^2 + (1 - 2i)x - 1 - i$. *Ans.* $(x - i)^2(x + 1 + i)$.

(b) $x^3 - (6 + 3\sqrt{5})x^2 + (27 + 12\sqrt{5})x - 38 - 17\sqrt{5}$. *Ans.* $(x - 2 - \sqrt{5})^3$.

(c) $x^4 - 6x^3 + 11x^2 - 6x + 1$.

(d) $x^6 + 3x^5 + 6x^4 + 7x^3 + 6x^2 + 3x + 1$.

(e) $x^8 - 4x^6 - 2x^4 + 12x^2 + 9$.

2. Solve each of the following equations, given that it has a repeated root.

(a) $x^4 + 2x^3 + 3x^2 + 4x + 2 = 0$.

(b) $x^3 + x^2 - (6 + 2\sqrt{2})x + 4\sqrt{2} = 0$.

(c) $x^4 - 4ix + 3 = 0$.

3. Show that the following polynomials have no repeated factors.

(a) $x^4 + 4x^2 - 4x - 3$.

(b) $x^5 - x^2 + 2$.

(c) $ax^n + b, \quad (ab \neq 0)$.

(d) $x^n - nx + 1, \quad (n \neq 2)$.

(e) $x^n - nx^{n-1} + 1, \quad (n \neq 2)$.

4. Find a condition which must be satisfied by the coefficients of each of the following polynomials in order that the polynomial have a repeated factor.

(a) $ax^2 + bx + c, \quad (a \neq 0)$. *Ans.* $b^2 - 4ac = 0$.

(b) $x^3 + 3Hx + G = 0$. *Ans.* $G^2 + 4H^3 = 0$.

(c) $x^4 + 4ax + b$. *Ans.* $b^3 - 27a^4 = 0$.

5. Show by an example that the second part of Theorem 3 becomes invalid if that part of the hypothesis is omitted which requires that B and B' be relatively prime.

21. Synthetic division. Synthetic division is a method of rapidly calculating the quotient and remainder of the division of a polynomial by a primary polynomial of the first degree. Let

$$Q(x) = q_0x^{n-1} + q_1x^{n-2} + \cdots + q_{n-2}x + q_{n-1}$$

be the quotient, and q_n the remainder, of the division of

$$A(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$$

by $x - h$, where h is a constant. Since

$$A(x) = (x - h)Q(x) + q_n,$$

$$\begin{aligned} a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n \\ &= (x - h)(q_0x^{n-1} + q_1x^{n-2} + \cdots + q_{n-2}x + q_{n-1}) + q_n \\ &= q_0x^n + (q_1 - hq_0)x^{n-1} + (q_2 - hq_1)x^{n-2} + \cdots \\ &\qquad + (q_{n-1} - hq_{n-2})x + q_n - hq_{n-1}. \end{aligned}$$

Equating coefficients of like powers of x, we obtain

$$q_0 = a_0,\ q_1 = a_1 + hq_0,\ q_2 = a_2 + hq_1,\ \cdots,$$
$$q_{n-1} = a_{n-1} + hq_{n-2},\ q_n = a_n + hq_{n-1}.$$

The a's and h being given, these equations show how the q's may be successively computed, the work being conveniently arranged as follows:

$$\begin{array}{l|llllll} & a_0 & a_1 & a_2 & \cdots & a_{n-1} & a_n \\ h & & hq_0 & hq_1 & \cdots & hq_{n-2} & hq_{n-1} \\ \hline & q_0 = a_0 & q_1 = a_1 + hq_0 & q_2 = a_2 + hq_1 & \cdots & q_{n-1} = a_{n-1} + hq_{n-2} & q_n = a_n + hq_{n-1}. \end{array}$$

The coefficients of $A(x)$ are written in order, 0 being substituted for any missing term. Multiply h by q_0, writing the product under a_1; adding, we obtain q_1. Now multiply h by q_1, writing the product under a_2; adding, we obtain q_2. This process is continued until it terminates naturally.

Where the numbers involved are fairly small, a_i and hq_{i-1} should be added mentally and the work exhibited as follows:

$$\begin{array}{llllll} & a_0 & a_1 & a_2 & \cdot & a_{n-1} & a_n \\ h. & q_0 & q_1 & q_2 & \cdot & q_{n-1} & q_n. \end{array}$$

Example. Divide $3x^5 - 8x^4 + x^2 - x + 3$ by $x - 2$.

Solution:

$$\begin{array}{|rrrrrr} 3 & -8 & 0 & 1 & -1 & 3 \\ 3 & -2 & -4 & -7 & -15 & -27. \end{array}$$

The quotient is $3x^4 - 2x^3 - 4x^2 - 7x - 15$, and the remainder is -27.

Explanation: Multiply 2 by 3 and add -8, obtaining -2; multiply 2 by -2 and add 0, obtaining -4; multiply 2 by -4 and add 1, obtaining -7; etc.

The remainder of the division of $A(x)$ by $x - h$ is, by the Remainder Theorem, $A(h)$. Synthetic division therefore provides a method of evaluating $A(h)$ which is frequently more expedient than that of substituting $x = h$ in $A(x)$.

EXERCISES

1. Divide

(a) $2x^3 - 3x^2 - 5x + 8$ by $x - 1$.
(b) $-x^4 + 9x^3 - 2x^2 + 10$ by $x + 1$.
(c) $3x^5 + x - 6$ by $x + 2$.
(d) $x^3 + (3 - 2i)x^2 + (1 + i)x - 4i$ by $x - i$.
(e) $x^4 + 3x^3 - 2x + 7$ by $x + 3$.
(f) $-4x^3 + 4x^2 - x - 5$ by $x - \frac{1}{2}$.

2. Find the value of $x^4 + x^3 - 3x^2 - 8x + 6$ for $x = 1, -1, 2, -3, 1 - i$.

3. Find the value of $-x^3 + 2x - 6$ for $x = 2, -4, 2 - \sqrt{3}$.

22. Taylor's Series. If $A(x)$ is a polynomial in a field R, $A(x + h)$ is a polynomial in $R(h)$, h being a new variable. Suppose that the expansion of $A(x + h)$ in powers of x is

$$(1) \qquad A(x + h) = b_n + b_{n-1}x + b_{n-2}x^2 + \cdots + b_0x^n,$$

where n is the degree of $A(x)$ and of $A(x + h)$, and the b's are functions of h which are to be determined.

Differentiating (1), we have

$$A'(x + h) = b_{n-1} + 2b_{n-2}x + 3b_{n-3}x^2 + \cdots + nb_0x^{n-1},$$

$$A''(x + h) = 2b_{n-2} + 6b_{n-3}x + 12b_{n-4}x^2 + \cdots + n(n - 1)b_0x^{n-2},$$

$$A^{(k)}(x + h) = k!b_{n-k} + (k + 1)!b_{n-k-1}x + \frac{(k + 1)!}{2!}b_{n-k-2}x^2 + \cdots + \frac{n!}{(n - k)!}b_0x^{n-k},$$

$$\cdots\cdots$$

$$A^{(n)}(x + h) = n!b_0.$$

Substituting $x = 0$ in each of these equations we have

$$b_n = A(h), b_{n-1} = A'(h), b_{n-2} = \frac{A''(h)}{2!},$$

$$b_{n-k} = \frac{A^{(k)}(h)}{k!}, \qquad , b_0 = \frac{A^{(n)}(h)}{n!}.$$

Therefore

$$(2) \quad A(x + h) = A(h) + A'(h)x + \frac{A''(h)}{2!}x^2 + \cdot \qquad + \frac{A^{(n)}(h)}{n!}x^n.$$

Replacing x by $x - h$, we have *Taylor's Series:*

$$(3) \quad A(x) = A(h) + A'(h)(x - h) + \frac{A''(h)}{2!}(x - h)^2 + \cdots$$
$$+ \frac{A^{(n)}(h)}{n!}(x - h)^n.$$

Taylor's Series for a polynomial involves only a finite number of terms because the $(n + 1)$th derivative of a polynomial of degree n vanishes.

It is found convenient, in practice, to compute the coefficients in (**3**) by synthetic division. It is evident from (**3**) that when $A(x)$ is divided by $x - h$ the remainder is $A(h)$ and the quotient is

$$Q_1(x) = A'(h) + \frac{A''(h)}{2!}(x - h) + \qquad \cdot + \frac{A^{(n)}(h)}{n!}(x - h)^{n-1}.$$

Again, the remainder obtained when $Q_1(x)$ is divided by $x - h$ is $A'(h)$ and the quotient is

$$Q_2(x) = \frac{A''(h)}{2!} + \frac{A'''(h)}{3!}(x - h) + \cdots + \frac{A^{(n)}(h)}{n!}(x - h)^{n-2};$$

etc. The coefficients in (**3**), being the remainders of certain successive divisions, are rapidly computed by synthetic division.

Example: Express $A(x) = 2x^4 - 3x^3 - x + 4$ in powers of $x - 2$.

Solution:

$$\begin{array}{r|rrrrr} \underline{2} & 2 & -3 & 0 & -1 & 4 \\ & & 1 & 2 & 3 & \mathbf{10} \\ & & 5 & 12 & \mathbf{27} & \\ & & 9 & \mathbf{30} & & \\ & \mathbf{2} & \mathbf{13} & & & \end{array}$$

The answer is

$$A(x) = 2(x - 2)^4 + 13(x - 2)^3 + 30(x - 2)^2 + 27(x - 2) + 10.$$

the problem been that of expanding $A(x+2)$, the calcula- vould have been the same, and the result

$$A(x+2) = 2x^4 + 13x^3 + 30x^2 + 27x + 10.$$

lanation: The second line indicates that when $A(x)$ is divided 2, the remainder is 10 and the quotient

$$Q_1(x) = 2x^3 + x^2 + 2x + 3.$$

ird line indicates that when $Q_1(x)$ is divided by $x - 2$, the ider is 27 and the quotient

$$Q_2(x) = 2x^2 + 5x + 12;$$

The remainders of the successive divisions are the required ients.

roots of the equation $A(x+h) = 0$ are obviously h less those of the equation $A(x) = 0$. The preceding discussion ore provides a solution of the problem of diminishing the of an equation by an assigned quantity.

EXERCISES

Express $2x^4 + x^3 - x^2 - 5x + 9$ in powers of $x + 3$

(a) by Taylor's Series.

(b) by synthetic division.

Given $A(x) = 3x^4 - 2x^3 + 6x^2 - 8x + 5$, express $A(x+2)$, 3), and $A(x + 2\sqrt{3})$ in powers of x

(a) directly, by substitution and expansion.

(b) by synthetic division.

Given $A(x) = x^3 + (1+i)x^2 - 2ix + 3$, express $A(x + 1 - i)$ in of x.

Given $A(x) = x^4 - (t+1)x^3 + t^2x^2 + (3t^2 + t)x - t^3 + t^2 - t$, ex- $(x + 2t)$ in powers of x.

Find the equation whose roots are 3 less than the roots of the equa- $- 12x^3 + 6x^2 - 7x + 13 = 0$.

Find the equation whose roots exceed the roots of the equation $11x^2 - x + 9 = 0$ by 4.

Determine h so that when the roots of the equation

$$a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n = 0$$

minished by h an equation is obtained in which the coefficient of

Ans. $h = -\dfrac{a_1}{na_0}$.

Diminish the roots of each of the following equations by a suitable

number so as to obtain an equation in which the coefficient of the second term is 0.

(a) $2x^3 + 6x^2 - x - 4 = 0.$
(b) $x^3 - 3x^2 + 8x + 12 = 0.$
(c) $x^4 - 8x^3 - 25x^2 - 36x + 18 = 0.$
(d) $x^3 - 3\sqrt{5}x^2 + (1 + \sqrt{5})x - 2 + 4\sqrt{5} = 0.$

9. Compute, by synthetic division, the numbers $c_0, \cdots, c_4$ such that

$$2x^4 - x^3 + 7x^2 - 8x + 11 = c_0x(x-1)(x-2)(x-3) + c_1x(x-1)(x-2) + c_2x(x-1) + c_3x + c_4.$$

10. Compute, by synthetic division, the numbers $c_0, \cdots, c_4$ such that

$$x^4 + 3x^3 - 7x^2 + 13x + 2 = c_0x(x+1)(x+2)(x+3) + c_1x(x+1)(x+2) + c_2x(x+1) + c_3x + c_4.$$

11. Show, with the aid of Taylor's Series, that if $x - r$ is an m-fold factor of $A(x)$, $A(x)$ and its first $m - 1$ derivatives vanish when $x = r$, while $A^{(m)}(r) \neq 0$.

12. Show that if r is a common root of the polynomials $A(x)$ and $B(x)$,

$$\left.\frac{A(x)}{B(x)}\right]_{x=r} = \left.\frac{A'(x)}{B'(x)}\right]_x$$

23. Construction of polynomials having assigned properties. A polynomial of degree $n - 1$ has n coefficients and may be determined by n conditions which are independent of and consistent with one another. Consider, for example, the *interpolation problem:* to construct a polynomial $A(x)$ of degree $\leq n - 1$, such that

$$A(x_i) = y_i \qquad (i = 1, \cdots, n), \tag{1}$$

where $x_1, \cdots, x_n; y_1, \cdots, y_n$ are given, no two of the x's being equal. If the polynomial

$$A(x) = a_0x^{n-1} + a_1x^{n-2} + \cdots + a_{n-2}x + a_{n-1}$$

has the stated properties, its coefficients must satisfy the equations

$$a_0x_i^{n-1} + a_1x_i^{n-2} + \cdots + a_{n-2}x_i + a_{n-1} = y_i \qquad (i = 1, \cdots, n). \tag{2}$$

This system of n linear equations in n unknowns (the a's) has a unique solution if and only if the determinant

$$\begin{vmatrix} 1 & x_1 & x_1^2 & \cdots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \cdots & x_2^{n-1} \\ & & & & \\ 1 & x_n & x_n^2 & & x_n^{n-1} \end{vmatrix} \tag{3}$$

does not vanish.

To prove that this determinant (which is called a *Vandermonde* determinant) does not vanish, let us regard the x's in (**3**) as independent variables. When $x_i = x_j$ $(i \neq j)$, two rows of V become identical and $V = 0$. Hence V is divisible by $x_i - x_j$ and therefore by

$$
(4)\quad \prod_{i>j}(x_i - x_j) = \begin{aligned}[t] &(x_n - x_1)(x_n - x_2) \cdots (x_n - x_{n-2})(x_n - x_{n-1}) \\ &\times (x_{n-1} - x_1)(x_{n-1} - x_2) \cdots (x_{n-1} - x_{n-2}) \\ &\quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ &\times (x_3 - x_2)(x_3 - x_1) \\ &\times (x_2 - x_1). \end{aligned}
$$

Since the right member of (**3**) and the right member of (**4**) have the same degree $\frac{1}{2}n(n - 1)$,

$$V = k \prod_{i>j} (x_i - x_j),$$

where k is a numerical constant. Now the coefficient of

$$x_2x_3^2 \qquad x_n^{n-1}$$

is 1 in both (**3**) and (**4**). Hence $k = 1$, and

$$(5)\qquad V = \prod_{i>j} (x_i - x_j).$$

It follows that V vanishes when and only when two of the x's are equal.

Since no two of the x's in (**1**) are equal, $V \neq 0$. The system of equations (**2**) therefore has a unique solution, which may be found by the usual methods of solving a system of linear equations.

There are other solutions of the interpolation problem. The following is due to Lagrange. We first construct the polynomial

$$(6)\qquad F(x) = (x - x_1)(x - x_2) \cdots (x - x_n),$$

whose roots are the given x's. As these roots are distinct,

$$F'(x_i) \neq 0, \qquad (i = 1, \cdots, n).$$

The polynomial

$$\frac{y_iF(x)}{(x - x_i)F'(x_i)}$$

vanishes when $x = x_k$ $(k \neq i)$, since $F(x_k) = 0$ while $x_k \quad x_i \neq 0$. On the other hand,

$$\left.\frac{y_iF(x)}{(x - x_i)F'(x_i)}\right]_{x = x_i} = \frac{y_iF'(x_i)}{F'(x_i)} = y_i.$$

We conclude that

$$(7)\quad A(x) = \sum_{i=1}^{n} \frac{y_i F(x)}{(x-x_i)\,F'(x_i)} \quad (\textit{Lagrange's interpolation-formula})$$

is the required polynomial; for its degree is $\leq n - 1$, and it assumes the value y_i when $x = x_i$.

Now suppose that $f(x)$ is a polynomial of unspecified degree satisfying the equations

$$(8)\qquad f(x_i) = y_i \qquad (i = 1, \cdots, n)$$

similar to (1). The polynomial $f(x) - A(x)$ vanishes when $x = x_1$, $x = x_2, \cdots, x = x_n$ and is therefore divisible by the polynomial $F(x)$ defined by (6). Hence

$$(9)\qquad f(x) = A(x) + T(x)F(x),$$

where $T(x)$ is a polynomial. Conversely, if $T(x)$ is an arbitrary polynomial, every member of the system of polynomials (9) satisfies the conditions (8).

Example. Construct a polynomial $f(x)$ of lowest possible degree such that

$$f(-2) = 11, f(-1) = -11, f(0) = -5, f(1) = -1, f'(1) = 5.$$

We first construct a polynomial $A(x)$ of degree ≤ 3 satisfying

$$A(-2) = 11,\ A(-1) = -11,\ A(0) = -5,\ A(1) = -1.$$

In applying Lagrange's interpolation-formula we have

$$\begin{aligned} F(x) &= (x+2)(x+1)x(x-1) = x^4 + 2x^3 - x^2 - 2x, \\ F'(x) &= 4x^3 + 6x^2 - 2x - 2, \\ F'(-2) &= -6,\ F'(-1) = 2,\ F'(0) = -2,\ F'(1) = 6. \end{aligned}$$

Hence, by (7),

$$\begin{aligned} A(x) &= \frac{11}{-6}(x+1)x(x-1) + \frac{-11}{2}(x+2)x(x-1) \\ &\qquad + \frac{-5}{-2}(x+2)(x+1)(x-1) + \frac{-1}{6}(x+2)(x+1)x \\ &= -5x^3 - x^2 + 10x - 5. \end{aligned}$$

By (9), the lowest degree $f(x)$ can have is 3, in which case $T(x) = 0$ and $f(x) = A(x)$. But $A'(1) = -7$, whereas it is required that $f'(1) = 5$. Hence $f(x)$ cannot be of degree 3. Assuming that the

degree of $f(x)$ is 4, $T(x)$ must be a constant t, and

$$f(x) = -5x^3 - x^2 + 10x - 5 + t(x^4 + 2x^3 - x^2 - 2x),$$
$$f'(x) = -15x^2 - 2x + 10 + t(4x^3 + 6x^2 - 2x - 2).$$

The condition $f'(1) = 5$ yields $t = 2$. The required polynomial is therefore

$$f(x) = 2x^4 - x^3 - 3x^2 + 6x - 5.$$

EXERCISES

1. Construct a polynomial $A(x)$ of lowest possible degree such that
(a) $A(0) = 0,\ A(1) = -1,\ A(-1) = 3$.
(b) $A(-1) = 0,\ A(0) = 5,\ A(2) = 1,\ A(3) = 0$.
(c) $A(0) = 1,\ A(1) = 2,\ A(2) = 5,\ A(3) = 10$.
(d) $A(1) = 1,\ A(2) = 0,\ A(3) = 0,\ A(4) = 0$.
(e) $A(i) = 1 + i,\ A(-i) = 1 - i,\ A(3) = 2$.
(f) $A(0) = t,\ A(1) = t^2 - 1,\ A(-1) = t^2 - 1$.

2. Construct a polynomial $f(x)$ of lowest possible degree such that
(a) $f(-1) = -4,\ f(0) = -1,\ f(1) = 4,\ f'(2) = -14$.
(b) $f(-2) = 5,\ f(-1) = 0,\ f(1) = -2,\ f(2) = 15,\ f'(0) = -3$.

3. Construct a *primary* polynomial $f(x)$ of lowest possible degree such that
(a) $f(0) = -7,\ f(1) = -7,\ f(2) = 9$.
(b) $f(-2) = 1;\ f(3) = -4,\ f(5) = 8$.
(c) $f(-1) = -2,\ f(0) = -2,\ f(1) = 0,\ f(2) = 16$.

4. With the notation of the text, show that

(a) $$F'(x) = \sum_{i=1}^{n} \frac{F(x)}{x - x_i}.$$

(b) $$\sum_{i=1} \frac{F(x)}{(x - x_i)F'(x_i)} \quad 1.$$

(c) $F'(x_1) \quad (x_1 - x_2)(x_1 - x_3) \cdots (x_1 - x_n)$.

(d) $V^2 \quad (-1)^{\frac{1}{2}n(n-1)} F'(x_1)F'(x_2) \cdots F'(x_n)$.

5. Show that if ϵ is a primitive nth root of unity,

$$\sum_{k=0}^{n-1} \frac{\epsilon^k(x^n - 1)}{x - \epsilon^k} \quad nx^2, \qquad (n > 2).$$

CHAPTER IV

THEORY OF EQUATIONS IN THE FIELD OF RATIONAL NUMBERS

24. A program for the study of the Theory of Equations. The concept of a field suggests a significant program for the study of the Theory of Equations. The first part of this program was partly developed in the two preceding chapters and will be resumed in Chapter VI. Its purpose is *to discover all theorems concerning polynomials and equations which are valid in all fields.* The realization of this goal, even in part, results in a great economy of thought, as duplications of demonstrations are avoided thereby.

There are, however, many theorems concerning polynomials and equations which are valid and significant in a certain field but are false or even meaningless in other fields.* This is due to the fact that a particular field may have certain peculiar properties not possessed by all fields, from which deductions may be made that are inapplicable to all fields. These remarks lead to a formulation of the second part of the program: *to discover those theorems which are valid in a selected field (or class of fields) and which are invalid or meaningless in other fields.*

In this chapter the field of rational numbers (which merits special attention because it is a subfield of every number-field) is the selected field; in the next chapter the field of real numbers is the subject of detailed investigation.

25. Properties of integers. In studying the Theory of Equations in a particular field, particular emphasis must be placed on those properties possessed by the elements of the field that serve to distinguish the field from other fields. We therefore remark, at the risk of repetition, that the field $R(1)$ consists of all numbers of the form p/q, where p and q are integers and $q > 0$. Without loss of generality, we shall suppose the numerator and denominator relatively prime, so that the fraction is reduced to its lowest terms.

* For example, the Fundamental Theorem of Algebra (every non-constant polynomial has a root) is valid in the field of complex numbers, but is invalid in the field of real numbers. On the other hand, Theorem 1 of this chapter is utterly meaningless when applied to the field of complex numbers.

Since a rational number is essentially an ordered pair of integers, the properties of integers investigated in Arithmetic may be expected to play a prominent part in this chapter. We therefore state explicitly the following arithmetical theorems to which we shall have occasion to refer:

1. The sum, difference, and product of two or more integers is an integer.

2. If the product ab of two integers a and b is divisible by the integer c, and a and c are relatively prime, then b is divisible by c.

26. Determination of rational roots. One of the general problems of the Theory of Equations in a field is: to find all the roots in the field of a given equation in the field. We do not demand an explicit formula for the roots of an arbitrary equation in the field in terms of its coefficients. The problem is considered solved if a method is provided for finding the roots by means of a *finite* number. of calculations. The following theorem provides a complete solution of this problem for the field of rational numbers.

THEOREM 1. *If a rational number, reduced to its lowest terms, is a root of an equation with integral coefficients, the numerator of the number is a divisor of the constant term of the equation, and the denominator is a divisor of the leading coefficient.*

Let

$$a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n = 0$$

be the equation and p/q the root in question. By hypothesis the a's are integers and p and q are relatively prime. Substituting $x = p/q$ in the equation, we obtain

$$a_0p^n + a_1p^{n-1}q + \qquad + a_{n-1}pq^{n-1} + a_nq^n = 0.$$

Dividing by p, we have

$$^{-1} + a_1p^{n-2}q + \qquad + a_{n-1}q^{n-1} + \frac{a_nq^n}{p} = 0.$$

By Property 1 of § 25, a_nq^n/p is an integer. Since p and q^n are relatively prime, a_n is divisible by p by Property 2.

In a similar manner we infer from the equation

$$\frac{a_0p}{q} + a_1p^{n-1} + \cdots + a_{n-1}pq^{n-2} + a_nq^{n-1} = 0$$

that a_0 is divisible by q.

An equation in $R(1)$ may be transformed into one having only

integral coefficients by multiplying the equation by a suitable integer. Since no root of the equation is altered thereby, there is no loss of generality in supposing that an equation in $R(1)$ has integral coefficients. The leading coefficient may be supposed to be different from 0 in any case. If the final coefficient is 0, 0 is a root of the equation. If 0 is an m-fold root, an equation whose final coefficient is different from 0 is obtained on removing the factor x^m.

We now suppose we have an equation with integral coefficients, whose leading and final coefficients are different from 0. Since every integer, except 0, has only a finite number of divisors, Theorem 1 limits the problem of finding the rational roots of the equation to a finite number of trials. The number of trials depends upon the number of divisors of the leading and final coefficients of the equation. Several devices for minimizing the number of necessary calculations are described in the following illustrative example.

Example. Examine the equation

$$4x^5 + 16x^4 + 9x^3 - 35x^2 - 51x - 18 = 0$$

for rational roots.

The only possible rational roots are those numbers whose numerators are divisors of 18 and whose denominators are divisors of 4, viz., 1, 2, 3, 6, 9, 18, $\frac{1}{2}$, $\frac{3}{2}$, $\frac{9}{2}$, $\frac{1}{4}$, $\frac{3}{4}$, $\frac{9}{4}$, and their negatives. Denoting any one of these numbers by r, and the left member of the equation by $f(x)$, we divide $f(x)$ by $x - r$; if a zero remainder is obtained, r is a root. The necessary calculations are most conveniently performed by synthetic division, the work being exhibited as follows:

	4	16	9	−35	−51	−18
1		20	29	−6	−57	−75
2		24	57	79	107	196
−1		12	−3	−32	−19	1
−2	4	8	−7	−21	−9	0
−3		−4	5	−36	99	
$\frac{1}{2}$		10	−2	−22	−20	
$\frac{3}{2}$		14	14	0	−9	
$-\frac{1}{2}$		6	−10	−16	−1	
$-\frac{3}{2}$	4	2	−10	−6	0	
	2	1	−5	−3		
$-\frac{3}{2}$		−2	−2	0		

Explanation: We first examine the equation for positive integral roots, the only possibilities being the positive divisors of 18. On dividing by $x - 2$, we observe that the numbers obtained (the coefficients of the quotient, and the remainder) all have the same sign and discard all numbers larger than 2 as possible roots (in particular 3, 6, 9, and 18). This rule will be justified in the next chapter. Turning to the negative divisors of 18, we find that -2 is a root, and that

$$f(x) = (x + 2)(4x^4 + 8x^3 - 7x^2 - 21x - 9).$$

All other roots of the proposed equation must be roots of the *depressed equation*

$$4x^4 + 8x^3 - 7x^2 - 21x - 9 = 0.$$

Having found that the proposed equation has no positive integral root, it is unnecessary to examine the depressed equation for positive integral roots: we simply *continue* our synthetic divisions, employing the depressed equation instead of the proposed equation.

After a root r has been found, the depressed equation should be examined with a view to determining whether it also has r as a root; if so, r is a multiple root of the proposed equation. In the present example, no such examination is necessary because 2 is not a divisor of the constant term of the depressed equation. We therefore proceed to -3, and here observe that the signs of the numbers obtained alternate; all smaller numbers (-9 in particular) are accordingly discarded as possible roots. This rule will also be justified in the next chapter.

We next turn our attention to the possible roots which have 2 as a denominator. We find that $-\frac{3}{2}$ is a root, and that the new depressed equation is

$$4x^3 + 2x^2 - 10x - 6 = 0.$$

After removing the common factor 2 from the coefficients of this equation, $-\frac{3}{2}$ is tried again and found to be a root. We now have the quadratic equation

$$2x^2 - 2x - 2 = 0,$$

or

$$x^2 - x - 1 = 0,$$

which should be solved directly. Its roots are $(1 \pm \sqrt{5})/2$, which are irrational.

The proposed equation therefore has exactly three rational roots: -2, $-\frac{3}{2}$, $-\frac{3}{2}$.

EXERCISES

1. Examine the following equations for rational roots:

(a) $x^3 + 3x^2 - 4x - 12 = 0$.
(b) $x^4 - 3x^3 + 10x^2 - 16x = 0$.
(c) $x^4 + 5x^3 + 9x^2 + 8x + 4 = 0$.
(d) $4x^4 - 8x^3 + 17x^2 - 13x + 3 = 0$.
(e) $12x^3 - 20x^2 - x + 6 = 0$.
(f) $6x^4 + 7x^3 - 7x^2 - 3x + 2 = 0$.
(g) $3x^5 - 2x^4 + 3x - 2 = 0$.

2. Show that

$$\sqrt[3]{2 + \tfrac{10}{9}\sqrt{3}} + \sqrt[3]{2 - \tfrac{10}{9}\sqrt{3}} \qquad \text{(real cube roots)}$$

is a rational number in disguise. [Find a cubic equation satisfied by this number. See p. 20, Example 5.]

3. Show that $\sqrt{2}$, $\sqrt[3]{5}$, $\sqrt{3} + \sqrt{5}$, and $\sqrt[3]{1 + \sqrt{2}} + \sqrt[3]{1 - \sqrt{2}}$ are irrational numbers.

4. Find three consecutive integers the sum of whose reciprocals is $\frac{47}{60}$.

5. By what number h must each of the roots of the equation

$$x^3 + 2x^2 - 11x - 8 = 0$$

be increased in order that the product of the increased roots be 4?

6. Find the dimensions of a rectangular box having a volume of 40 cu. ft. if the length exceeds the width by 1 ft. and the depth by 3 ft.

7. (a) Show that the lengths of the three edges of a rectangular box satisfy the equation

$$x^3 - \sqrt{l^2 + A}\,x^2 + \tfrac{1}{2}Ax - V = 0,$$

where l is the length of the diagonal of the box, A its total area, and V its volume.

(b) Find the dimensions of a box, given $l = 7$, $A = 72$, $V = 36$.

8. Find three numbers whose sum is 8, whose product is 12, and the sum of whose squares is 26. [Find a cubic equation satisfied by the three numbers, using the relations between the roots and coefficients.]

9. Find five numbers in geometric progression whose sum is $\frac{121}{9}$ and whose product is 1.

10. Determine k so that one root of the equation

$$x^3 + 9x^2 + kx + 24 = 0$$

shall be twice another; and find the roots.

11. Find all values of k for which the polynomial

$$x^3 - 3kx + 2k + 8$$

has a repeated factor. *Ans.* $k = 4, \; -3 \pm \sqrt{-7}$

12. Prove the following theorem, which is analogous to Theorem 1.

THEOREM 2. *If $P(y)$ and $Q(y)$ are relatively prime polynomials in a field R, and $P(y)/Q(y)$ is a root of the equation.*

$$A_0(y)x^n + A_1(y)x^{n-1} + \cdots + A_{n-1}(y)x + A_n(y) = 0,$$

whose coefficients are polynomials in R, then $P(y)$ is a divisor of $A_n(y)$ and $Q(y)$ is a divisor of $A_0(y)$.

13. Solve the equation

$$(y + 1)x^3 + (2y^3 + 5y^2 + 4y)x^2 + (6y^4 + 8y^3 - 3y - 1)x \\ - 6y^3 - 2y^2 = 0$$

for x with the aid of Theorem 2. *Ans.* $x = -2y^2, \; -3y - 1, \; \frac{1}{\quad + 1}$

14. Show that the equation

$$4x^3 - 3x - y = 0$$

is irreducible in the field $R(y)$ of rational functions, with coefficients in the field of complex numbers, of the variable y.

15. Why would a theorem analogous to Theorem 1 be meaningless in the field of complex numbers?

27. Reducibility of polynomials. Another problem of the Theory of Equations in a field is: to determine whether a given polynomial is reducible or irreducible in the field. This problem was solved completely by Kronecker for the field of rational numbers. We shall not describe Kronecker's solution here, as the required computations are usually prohibitive. Instead, we shall prove a few theorems which are useful in discussing the irreducibility of polynomials in $R(1)$.

By direct multiplication we find that if

$$A(x) = B(x)C(x), \tag{1}$$

where

$$\begin{aligned} A(x) &= a_0x^n + a_1x^{n-1} + \quad\quad + a_{n-1}x + a_n, \\ B(x) &= b_0x^r + b_1x^{r-1} + \quad\quad + b_{r-1}x + b_r, \qquad (a_0b_0c_0 \neq 0) \\ C(x) &= c_0x^s + c_1x^{s-1} + \quad\quad + c_{s-1}x + c_s, \end{aligned} \tag{2}$$

then $r + s = n$, and

$$
\begin{aligned}
a_0 &= b_0c_0, \\
a_1 &= b_0c_1 + b_1c_0, \\
a_2 &= b_0c_2 + b_1c_1 + b_2c_0, \\
&\cdots\cdots \\
a_s &= b_0c_s + b_1c_{s-1} + \cdots, \qquad (3) \\
&\cdots\cdots \\
a_{n-2} &= b_{r-2}c_s + b_{r-1}c_{s-1} + b_rc_{s-2}, \\
a_{n-1} &= b_{r-1}c_s + b_rc_{s-1}, \\
a_n &= b_rc_s.
\end{aligned}
$$

The student should carefully note the law of formation of these equations. The general equation of the set (3) is

$$(4) \qquad a_k = b_0c_k + b_1c_{k-1} + \cdots + b_{k-1}c_1 + b_kc_0,$$

in which all the b's with subscripts $> r$ and all the c's with subscripts $> s$ are to be equated to 0. This equation may also be written

$$(5) \quad a_{u+v} = b_uc_v + b_{u-1}c_{v+1} + b_{u-2}c_{v+2} + \cdots + b_{u+1}c_{v-1} + b_{u+2}c_{v-2} + \cdots,$$

the series terminating naturally.

A polynomial with integral coefficients is *primitive* if the g.c.d. of its coefficients is 1; in the contrary case the polynomial is *imprimitive.*

THEOREM 3. (GAUSS.) *The product of two primitive polynomials is a primitive polynomial.*

With the preceding notation, let $B(x)$ and $C(x)$ be primitive polynomials, and suppose that, contrary to the theorem, $A(x)$ is imprimitive. Then there exists a prime number p which is a divisor of all the a's. Since $B(x)$ and $C(x)$ are primitive polynomials, each of them has at least one coefficient which is not divisible by p. Let b_u and c_v be the coefficients of smallest subscripts of $B(x)$ and $C(x)$ respectively that are not divisible by p. Evidently, $u \geq 1$ and $v \geq 1$. Since p is a divisor of each of the integers a_{u+v}, b_{u+1}, b_{u+2}, $\cdots$, c_{v+1}, c_{v+2}, $\cdots$, it follows from (5) that p is a divisor of b_uc_v, and hence of either b_u or c_v. This being contrary to assumption, it follows that $A(x)$ is a primitive polynomial.

THEOREM 4. (GAUSS.) *A polynomial with integral coefficients, which is reducible in $R(1)$, can be expressed as the product of two polynomials with integral coefficients.*

Let $A(x)$ be the given polynomial. By hypothesis

$$A(x) = B(x)C(x),$$

where $B(x)$ and $C(x)$ are polynomials in $R(1)$ of degree ≥ 1. Let l_1 and l_2 be the least common denominators of the coefficients of $B(x)$ and $C(x)$ respectively. Then

$$B_1(x) = l_1B(x), \qquad C_1(x) = l_2C(x)$$

are polynomials with *integral* coefficients, and

$$l_1l_2A(x) = B_1(x)C_1(x).$$

Let d_a, d_b, and d_c be the g.c.d.'s of the coefficients of $A(x)$, $B_1(x)$, and $C_1(x)$ respectively. Then

$$\frac{A(x)}{d_a}, \qquad B_2(x) = \frac{B_1(x)}{d_b}, \qquad C_2(x) = \frac{C_1(x)}{d_c}$$

are *primitive* polynomials, and

$$\frac{d_al_1l_2}{d_bd_c}\cdot\frac{A(x)}{d_a} \qquad \frac{B_1(x)}{d_b}\cdot\frac{C_1(x)}{d_c} \qquad B_2(x)C_2(x).$$

By Theorem 3, the left member is a primitive polynomial; therefore

$$d_al_1l_2 \quad 1.$$

Hence

$$\begin{aligned} A(x) &= \frac{B_1(x)C_1(x)}{l_1l_2} = \frac{d_bB_2(x)\cdot d_cC_2(x)}{l_1l_2} \\ &= \frac{d_bd_c}{l_1l_2}\cdot B_2(x)C_2(x) = [d_aB_2(x)]C_2(x), \end{aligned}$$

where $d_aB_2(x)$ and $C_2(x)$ are polynomials with integral coefficients, whose degrees are equal to those of $B(x)$ and $C(x)$ respectively.

THEOREM 5. (EISENSTEIN.) *A polynomial*

$$A(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$$

with integral coefficients is irreducible in $R(1)$ if there exists a prime number p which is a divisor of all the a's except a_0, and p^2 is not a divisor of a_n.

If possible, let $A(x) = B(x)C(x)$, where $B(x)$ and $C(x)$ are polynomials of degree ≥ 1 with integral coefficients (Theorem 4). Let (**1**) be the explicit forms of these polynomials.

Since a_n is divisible by p but not by p^2, one and only one of the integers b_r and c_s is divisible by p (see the last of equations (**3**)). We suppose that b_r is divisible by p while c_s is not divisible by p. It follows from the next to the last of equations (**3**) that, since a_{n-1} and b_r are divisible by p while c_s is not divisible by p, b_{r-1} is divisible by p. In the same way, it follows from the immediately preceding equation that b_{r-2} is divisible by p. Continuing thus, we finally infer from

$$a_s = b_0c_s + b_1c_{s-1} + \cdots$$

that b_0 is divisible by p. It follows from the first of equations (**3**) that a_0 is divisible by p, contrary to assumption. Therefore $A(x)$ is irreducible in $R(1)$.

Example. Prove that the polynomial

$$x^{p-1} + x^{p-2} + \qquad + x + 1, \qquad (p \text{ prime})$$

is irreducible in $R(1)$.

Denoting this polynomial by $F(x)$, we have

$$F(x) = \frac{x^p - 1}{x - 1}$$

The roots of $F(x)$ are therefore the primitive pth roots of unity. Eisenstein's Theorem cannot be applied directly to $F(x)$, since all its coefficients are 1. However, $F(x)$ and $F(x + 1)$ are simultaneously reducible or irreducible. For if $F(x) = F_1(x)F_2(x)$, $F(x + 1) = F_1(x + 1)F_2(x + 1)$; and if $F(x + 1) = G_1(x)G_2(x)$, $F(x) = G_1(x - 1)G_2(x - 1)$. Now

$$F(x + 1) = \frac{(x + 1)^p - 1}{(x + 1) - 1} \quad (x + 1)^p - 1$$
$$x^{p-1} + px^{p-2} + \frac{p(p - 1)}{2}x^{p-3} + \cdots + \frac{p(p - 1)}{2}x + p,$$

each of whose coefficients, except the first, is divisible by p, while the last is not divisible by p^2. Therefore $F(x)$ is irreducible in $R(1)$.

EXERCISES

Show that the following polynomials are irreducible in $R(1)$.

1. $x^n - p$, where p is a prime number.

2. $x^4 + 4k + 1$, where k is any integer. [Replace x by $x + 1$.]

3. $x^4 + 4x + 1$.

4. $2x^4 + 5x^3 + 6x^2 + 5x - 4$.

5. $3x^4 + 3x + 1$. [Replace x by $1/x$.]

6. $x^p + px + 1$, where p is a prime > 2.

7. $1 + x + \dfrac{x^2}{2!} + \dfrac{x^3}{3!} + \cdots + \dfrac{x^p}{p!}$, ($p$ prime).

8. $x^n + (1 + x)^m + (1 - x)^m$, $(m \leq n)$.

CHAPTER V

THEORY OF EQUATIONS IN THE FIELD OF REAL NUMBERS

28. Introduction. As noted in § 24, the first step in the preparation of the study of the Theory of Equations in a particular field consists of a declaration and elucidation of those properties of the field which distinguish the field from other fields. We therefore remark at this point that the field of real numbers is *ordered* and *compact*. These properties will be fully described in the next two sections.

The field of real numbers is not the only field which is ordered nor the only field which is compact. For example, the field of rational numbers is ordered and the field of complex numbers is compact. But the field of real numbers is the only number-field which is *both* ordered and compact. The reader should bear this statement in mind throughout this chapter, observing how these properties enter into our investigations and why the results obtained are invalid or meaningless in other fields. Moreover, it may be pointed out that it is because the field of real numbers is ordered and compact that this field plays an important rôle in other branches of mathematics such as Analytic Geometry and the Calculus.

29. Ordered fields. Any two distinct real numbers have the property that one is *less than* the other. The real numbers may therefore be arranged in a definite *order* by agreeing that a is to *precede* b if $a < b$; then $b > a$, and b is said to *succeed* a. The ordering of the real numbers has the following properties (*axioms of order*):

1. If $a < b$, then $a \neq b$.
2. If $a \neq b$, then either $a < b$ or $a > b$.
3. If $a < b$ and $b < c$, then $a < c$.
4. If $a < b$, then $a + c < b + c$.
5. If $a > 0$ and $b > 0$, then $ab > 0$.

Here a, b, and c are real numbers. In reading the axioms of order

the symbols $<$ and $>$ should be read "precedes" and "succeeds" respectively rather than "is less than" and "is greater than" respectively.

An ordered field is one for which it is possible to define the relation $<$ and the converse relation $>$ for any two elements of the field so that the preceding axioms of order are verified for any elements a, b, and c of the field.

Every subfield of the field of real numbers is clearly an ordered field. But the field of complex numbers cannot be ordered. For in the contrary case we should have either $i > 0$ or $i < 0$. If $i > 0$, $i^2 > 0$ by Axiom 5; or $-1 > 0$. Applying Axiom 5 again, we have $1 > 0$. On the other hand, adding 1 to both members of the inequality $-1 > 0$, which is permissible by Axiom 4, we obtain $0 > 1$. We now have $1 > 0$ and $0 > 1$, from which it follows by Axiom 3 that $0 < 0$, which violates Axiom 1. The assumption that $i < 0$ also leads to a contradiction. Therefore no field which includes the number i can be ordered.

30. Compactness. An infinite sequence of real numbers

$$(1) \qquad a_1, a_2,$$

converges if, corresponding to *any* positive number ϵ, an integer n can be found such that

$$(2) \qquad u_{n+p} \quad a_n \mid < \epsilon$$

for every $p \geq 0$; otherwise the sequence *diverges*. It is to be emphasized that the choice of n depends upon ϵ, whereas p is independent of ϵ. If a sequence converges it is possible to find a term of the sequence such that the difference between this term and any subsequent term is numerically less than any preassigned positive number, no matter how small.

The infinite series

$$c_1 + c_2 + c_3 + \cdots$$

of real terms *converges* or *diverges* according as the sequence

$$c_1, c_1 + c_2, c_1 + c_2 + c_3, \cdots$$

converges or diverges.

The sequence (1) has the *limit* l if, corresponding to any positive

number ϵ, an integer n_1 can be found such that

$$(3) \qquad | l - a_n | < \epsilon$$

for *every* integer $n \geq n_1$.*

As a simple example, let us consider the sequence

$$1, \tfrac{1}{2}, \tfrac{1}{3}, \tfrac{1}{4}, \cdots.$$

To prove that the sequence converges we must produce, corresponding to any $\epsilon > 0$, an integer n such that

$$\frac{1}{n+p} \quad n \quad < \epsilon$$

for every integer $p \geq 0$. Choose n as the smallest integer $> 1/\epsilon$. Then

$$0 \leq \frac{1}{n} - \frac{1}{n+p} < \frac{1}{n} < \epsilon.$$

Hence, for every $p \geq 0$,

$$| n + p \qquad < \epsilon.$$

The sequence therefore converges.

The limit of the sequence is evidently 0. To prove that this is the case, we must produce an integer n_1 corresponding to any given $\epsilon > 0$, such that $| 0 - 1/n | < \epsilon$ for every $n \geq n_1$. Choose n_1 as the smallest integer $> 1/\epsilon$. Then, if $n \geq n_1$,

$$0 - \frac{1}{n} \quad \frac{1}{n} \leq \frac{1}{n_1} < \epsilon.$$

The property of compactness possessed by the field of real numbers is expressed by the

THEOREM 1. *If a sequence of real numbers converges, there exists a real number which is the limit of the sequence.*†

The point is that the field of real numbers does not have to be enlarged in order to admit those numbers which are limits of convergent sequences of real numbers: all such limits are already in the field. This is not the case for any subfield of the field of real

* The preceding definitions are readily extended to the field of complex numbers.

† A similar theorem is valid in the field of complex numbers, which is therefore a compact field.

numbers. It is not true that the limit of a convergent sequence of rational numbers is a rational number. For example, in the process of extracting the square root of 2 a convergent sequence of *rational* numbers

$$1, 1.4, 1.41, 1.414, 1.4142, \cdots$$

is obtained, whose limit is an irrational number, namely $\sqrt{2}$. The property of compactness distinguishes the field of real numbers from its subfields.

A rigorous proof of Theorem 1 is beyond the scope of this book, requiring a close examination of the axioms of the real number system, and will therefore be omitted.

31. Continuity. A function of a real variable x is continuous at $x = c$ if, corresponding to any given $\epsilon > 0$, a $\delta > 0$ can be found such that

$$|f(x) - f(c)| < \epsilon$$

for every x satisfying $|x - c| \leq \delta$. This definition expresses with precision the idea that a continuous function varies slightly when its argument varies slightly.

A function $f(x)$ is continuous in an interval if it is continuous for every value of x in the interval. If $f(x)$ is continuous in an interval, the curve $y = f(x)$ is continuous in the interval. This may be taken as a definition of continuity of a curve in an interval. However, the reader has intuitive notions as to what a continuous curve is, and he should satisfy himself that the preceding analytic definition conforms to his intuitive notions.

THEOREM 2. *A polynomial in the field of real numbers is a continuous function of its argument.*

If $A(x)$ is a polynomial of degree n,

$$A(x) - A(c) = (x - c)A'(c) + (x - c)^2\frac{A''(c)}{2!} + \cdots + (x - c)^n\frac{A^{(n)}(c)}{n!}.$$

Let M be a positive number greater than the absolute value of each of the coefficients of the right member of this equation. Then

$$|A(x) - A(c)| < M|x - c|[1 + |x - c| + |x - c|^2 + \cdots + |x - c|^{n-1}].$$

The expression in the brackets is a geometric progression whose sum is

$$\frac{1 - |x - c|^{\cdot}}{1 - |x - c|}, \text{ which is less than } \frac{1}{1 - |x - c|} \text{ if } |x - c| < 1.$$

Corresponding to any assigned $\epsilon > 0$, let $\delta = \epsilon/(M + \epsilon)$ which is clearly < 1. Hence for every x such that $|x - c| \leq \delta$,

$$|A(x) - A(c)| < \frac{M|x - c|}{1 - |x - c|} < \frac{M\delta}{1 - \delta} = \epsilon.$$

It follows from the definition that $A(x)$ is continuous at $x = c$.

THEOREM 3. *If* $A(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$ *is a polynomial with real coefficients, then*

(1) $\quad A(\infty) = \lim_{x\to\infty} A(x) = +\infty$ *if* $a_0 > 0$, *and* $-\infty$ *if* $a_0 < 0$;

(2) $\quad A(-\infty) = \lim_{x\to-\infty} A(x) = +\infty$ *if* $(-1)^n a_0 > 0$, *and* $-\infty$ *if* $(-1)^n a_0 < 0$.

(1) means that if P is any preassigned positive number, no matter how large, a real number x_0 can be found such that for every $x \geq x_0$

$$A(x) > P \text{ if } a_0 > 0, \qquad A(x) < -P \text{ if } a_0 < 0.$$

(2) means that if P is any preassigned positive number, no matter how large, a real number x_0 can be found such that for every $x \leq x_0$

$$A(x) > P \text{ if } (-1)^n a_0 > 0, \qquad A(x) < -P \text{ if } (-1)^n a_0 < 0.$$

Hence, $A(x)$ has the same sign as a_0 for all sufficiently large positive values of x, and $A(x)$ has the same sign as $(-1)^n a_0$ for all sufficiently large negative values of x.

To prove the theorem, let

$$f(x) = a_1x + a_2x^2 + \cdots + a_nx^n,$$

so that

$$A(x) = x^n[a_0 + f(1/x)].$$

Since $f(0) = 0$ and $f(x)$ is continuous at $x = 0$, a $\delta > 0$ can be found corresponding to any preassigned $\epsilon > 0$ such that

$$|f(x)| < \epsilon \text{ for every } x \text{ such that } |x| < \delta.$$

Choose ϵ so that $0 < \epsilon < |a_0|$. Then $a_0 + \epsilon$ has the same sign as a_0. Hence $a_0 + f(1/x)$ has the same sign as a_0 for every x such that $|x| > 1/\delta$. The theorem now follows from the observation that

$$\lim_{x\to\infty} x^n \quad +\infty, \qquad \lim_{x\to-\infty} x^n = (-1)^n\infty.$$

32. The fundamental property of continuous functions.

THEOREM 4. *If $f(x)$ is continuous between $x = a$ and $x = b$ and y is a real number between $f(a)$ and $f(b)$, the equation $f(x) = y$ has at least one real root between a and b.*

The proof of this fundamental theorem will be omitted.* Let the reader interpret the theorem graphically and appeal to his intuitive notions of continuity.

EXERCISES

1. Show by an example that a false proposition is obtained when "real" is replaced by "rational" in Theorem 4.

2. Show that if $f(x)$ is a real continuous function between $x = a$ and $x = b$ and if $f(a)$ and $f(b)$ have opposite signs, the equation $f(x) = 0$ has at least one real root between a and b. Illustrate graphically.

3. Show that a polynomial with real coefficients, whose leading and final coefficients have opposite signs, has at least one positive root. Illustrate. [Apply Theorems 3 and 4.]

4. Show that every positive real number has exactly one positive real nth root, where n is any positive integer.

5. If $f(x) = x^2 + 3x - 5$, then $f(-2) = -7$ and $f(2) = 5$. According to Theorem 4 each of the equations

$$f(x) = -6,\ f(x) = -1,\ f(x) = 0,\ f(x) = 4$$

has a real root between -2 and $+2$. Verify by finding these roots.

6. Although $\tan \pi/4 = 1$ and $\tan 3\pi/4 = -1$, the equation $\tan x = 0$ has no real root between $\pi/4$ and $3\pi/4$. Explain.

7. Prove: *If*

$$f(x) = (x - r)^m g(x) \qquad (g(r) \neq 0)$$

where r is a real number and $g(x)$ is a polynomial with real coefficients—in other words, if r is a root of multiplicity m of $f(x)$—then $f(x)$ does or does not change sign in an interval containing r and in which $g(x)$ preserves its sign, according as m is odd or even.

* The reader who wishes to see what is involved in a rigorous proof of this theorem may consult G. H. Hardy, *A Course of Pure Mathematics*, third edition (1921), p. 179.

8. Prove: (a) *If $f(x)$ is a polynomial with real coefficients and $f(a)$ and $f(b)$ have opposite signs, then the equation $f(x) = 0$ has an odd number of roots between a and b, each multiple root being counted to its degree of multiplicity.*

(b) *If $f(a)$ and $f(b)$ have the same sign, the equation $f(x) = 0$ has no root or an even number of roots between a and b, each multiple root being counted to its degree of multiplicity.*

9. Prove: *Every polynomial of odd degree with real coefficients has at least one real root.* [Use Theorem 3 and Ex. 8 (a).]

10. Give examples of functions which do not have the property of polynomials described by Theorem 3.

33. Rolle's Theorem. Let x_1 and x_2 be two consecutive roots of a polynomial $f(x)$, so that $f(x)$ has no root between x_1 and x_2; and let x_1 be a root of multiplicity m_1 and x_2 a root of multiplicity m_2. Then

$$(1) \qquad f(x) = (x - x_1)^{m_1}(x - x_2)^{m_2}g(x),$$

$g(x)$ being a polynomial which does not change sign between x_1 and x_2 inclusive. Differentiating (**1**) we obtain

$$\begin{aligned}(2) \quad f'(x) &= (x - x_1)^{m_1}(x - x_2)^{m_2}g'(x) \\ &\quad + [m_1(x - x_1)^{m_1-1}(x - x_2)^{m_2} + m_2(x - x_1)^{m_1}(x - x_2)^{m_2-1}]g(x) \\ &= (x - x_1)^{m_1-1}(x - x_2)^{m_2-1}F(x),\end{aligned}$$

where

$$F(x) = m_1(x - x_2)g(x) + m_2(x - x_1)g(x) + (x - x_1)(x - x_2)g'(x).$$

Substituting $x = x_1$ and $x = x_2$ we obtain

$$(3) \quad F(x_1) = m_1(x_1 - x_2)g(x_1), \qquad F(x_2) = m_2(x_2 - x_1)g(x_2).$$

Since $g(x)$ has no root between x_1 and x_2 inclusive and preserves its sign in this interval, $F(x_1)$ and $F(x_2)$ have opposite signs by (**3**). Therefore $F(x)$ has an odd number of roots between x_1 and x_2. It follows from (**2**) that the same is true of $f'(x)$.

THEOREM 5. (ROLLE.) *Between two consecutive real roots of a polynomial with real coefficients there is an odd number of roots of its derivative, and hence at least one.*

Interpreted graphically, Rolle's Theorem asserts that the curve $y = f(x)$ has at least one maximum or minimum point between x_1 and x_2. The theorem is valid for any continuous real function of a real variable whose derivative exists throughout the interval $[x_1, x_2]$.

EXERCISES

1. Verify Rolle's Theorem for the polynomials

(a) $x^2 - 3x + 2$. (c) $x^4 - 1$.

(b) $x^3 - 6x^2 + 11x - 6$. (d) $x^3 + 2x^2 - 1$.

2. Show that at most one root of $f(x)$ lies between two consecutive roots of $f'(x)$.

3. Show that at most one real root of $f(x)$ is greater than the largest real root of $f'(x)$; and that at most one real root of $f(x)$ is less than the smallest real root of $f'(x)$.

4. Show that if $f(x)$ has r real roots, its kth derivative has at least $r - k$ real roots.

5. Show that if the kth derivative of $f(x)$ has exactly s real roots, $f(x)$ has at most $s + k$ real roots.

6. Show that the equation $x^3 - 3x^2 + 8x + 1 = 0$ has one negative and two imaginary roots.

7. Show that the equation $x^4 + x^3 + x^2 + x - 1 = 0$ has one positive, one negative, and two imaginary roots.

8. Show that the equation $x^5 + 5x + 1 = 0$ has one negative and four imaginary roots.

9. Show that if $a_1, a_2, \cdots, a_k (k \geq 2)$ are positive numbers, and $b_1, b_2, \cdots, b_k$ are real numbers, at least two of which are distinct, the equation

$$a_1(x + b_1)^n + a_2(x + b_2)^n + \cdots + a_k(x + b_k)^n = 0$$

has no real root if n is even and exactly one real root if n is odd.

10. Show that the equation

$$(x + 1)^n + (x - 1)^n - 3 = 0$$

has exactly one real root if n is odd and exactly two real roots if n is even.

11. Show that if x_1 and x_2 are two consecutive roots of a polynomial $f(x)$ with real coefficients, then $f'(x_1)$ and $f'(x_2)$ have opposite signs if neither vanishes. Illustrate graphically. [Use (2) and (3), observing that $m_1 = m_2 = 1$ and that $f'(x) = F(x)$.]

12. Show that if all the roots of a polynomial $f(x)$ are real and distinct, $f'(x)$ cannot have any multiple roots.

13. Assuming that Rolle's Theorem is true for continuous, differentiable functions of a real variable, show that the equation

$$x^2 - x \sin x - \cos x = 0$$

has exactly two real roots.

14. Show by an example that a false proposition is obtained when "real" is replaced by "rational" in Theorem 5.

15. The function $f(x) = x - 1/x$ vanishes for $x = \pm 1$ but its derivative $f'(x) = 1 + 1/x^2$ has no real root. Explain, and illustrate graphically.

16. Verify that ± 1 are roots of the polynomial

$$f(x) = x^3 + ix^2 - x - i.$$

Show that $f'(x)$ has no root between -1 and $+1$. Explain.

17. (a) Show that if $c_1, c_2, \cdots, c_n$ are distinct real numbers the equation

$$f(x) = (x - c_1)^{-1} + (x - c_2)^{-1} + \cdots + (x - c_n)^{-1} = 0$$

has $n - 1$ distinct real roots. [Observe that if

$$A(x) = (x - c_1)(x - c_2) \cdots (x - c_n),$$

then $f(x) = A'(x)/A(x)$.]

(b) Show that $f'(x)$ has no real root.

(c) Are these two results inconsistent with Rolle's Theorem?

34. Graphs of polynomials. The following example will serve as an illustration of the method of sketching the graph of a polynomial.

Example. Trace the curve

$$y = f(x) = 3x^4 - 2x^3 - 36x^2 + 36x - 8,$$

and derive therefrom information concerning the roots of $f(x) = 0$.

We have

$$f'(x) = 12x^3 - 6x^2 - 72x + 36.$$
$$f''(x) = 36x^2 - 12x - 72.$$

The roots of $f'(x) = 0$ are $\frac{1}{2}$, $\sqrt{6}$, and $-\sqrt{6}$, which are the abscissas of the critical points; the corresponding ordinates are $\frac{15}{16}$, $-116 + 24\sqrt{6} = -57.2$, and $-116 - 24\sqrt{6} = -174.8$ respectively. The roots of $f''(x) = 0$ are $(1 + \sqrt{73})/6 = 1.6$ and $(1 - \sqrt{73})/6 = -1.3$, which are the abscissas of the points of inflection; the corresponding ordinates are -30.4 and -98.5 respectively.

A *table of values* is now constructed:

x					y
0	3	-2	-36	36	-8
1		1	-35	1	-7
2		4	-28	-20	-48
3		7	-15	-9	-35
4		10	4	52	200
-1		-5	-31	67	-75
-2		-8	-20	76	-160
-3		-11	-3	45	-143
-4		-14	20	-44	168

The first row expresses the obvious fact that $f(0) = -8$. The values of $f(x)$ for $x = \pm 1, \pm 2, \cdots$ are found by synthetic division. We stop with $x = 4$ because all the numbers appearing in this row (including the initial 3 which it is unnecessary to write in each row) have the same sign. We stop with -4 because the numbers which follow it alternate in sign.

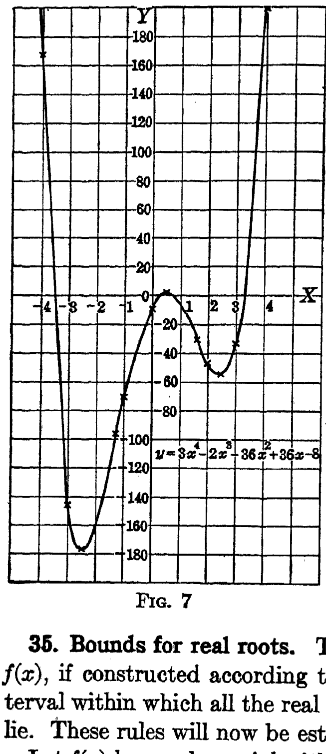

FIG. 7

These points, as well as the critical points and the points of inflection, are then plotted, the unit on the y-axis being taken as $\frac{1}{20}$th that on the x-axis in order that the graph may be kept within the available space. The graph (Fig. 7) is completed by connecting the points by a smooth curve.

It is seen from the graph that there are four real roots of $f(x) = 0$, one in each of the intervals $[-4, -3]$, $[0, \frac{1}{2}]$, $[\frac{1}{2}, 1]$, $[3, 4]$. The two real roots in the interval $[0, 1]$ would probably have been overlooked if the critical points had not been plotted.

35. Bounds for real roots. The table of values of a polynomial $f(x)$, if constructed according to the stated rules, provides an interval within which all the real roots of $f(x)$, if there are any, must lie. These rules will now be established.

Let $f(x)$ be a polynomial with real coefficients and degree n, and let c be a real number ≥ 0. Let q_n be the remainder and

$$Q(x) = q_0x^{n-1} + q_1x^{n-2} + \cdots + q_{n-2}x + q_{n-1}$$

the quotient of the division of $f(x)$ by $x - c$; and suppose that all the q's have the same sign. For definiteness we shall suppose that all the q's are positive. We have

$$f(x) = (x - c)Q(x) + q_n,$$

where $q_n = f(c)$ by the Remainder Theorem.

Let x_1 and x_2 be two real numbers such that $x_2 > x_1 > c$. Then

$$x_2 - c > x_1 - c > 0,$$

and

$$q_k x_2^{n-k-1} \geqq q_k x_1^{n-k-1} \qquad (k = 0,\ 1,\ \cdots,\ n-1).$$

Hence, by addition, $Q(x_2) > Q(x_1)$. It follows that

$$(x_2 - c)Q(x_2) + q_n > (x_1 - c)Q(x_1) + q_n,$$

or $f(x_2) > f(x_1)$. Therefore if x increases from any value $> c$ to a larger value, $f(x)$ remains positive and continually increases. Similarly, when all the q's are negative, if x increases from any value $> c$ to a larger value, $f(x)$ remains negative and continually decreases. Consequently $f(x)$ cannot vanish if $x > c$.

The rule for the lower bound of the real roots of $f(x)$ is obtained by applying the preceding result to the polynomial $f(-x)$, whose roots are the negatives of those of $f(x)$.

EXERCISES

1. Sketch the graphs of the following polynomials and locate their roots.

(a) $x^3 - 3x + 2$.
(b) $-2x^3 + 9x^2 - 12x + 4$.
(c) $2x^3 - 3x^2 + 6x + 2$.
(d) $x^3 - 3x^2 + 3x + 3$.
(e) $x^4 - 2x^3 - 2x^2 + 6x - 1$.
(f) $2x^4 - 4x^3 - 18x^2 + 15x - 3$.
(g) $x^4 - 4x^3 + 6x^2 + 28x + 17$.
(h) $3x^4 - 4x^3 + 6x^2 - 12x + 9$.
(i) $x^4 + 4x + 1$.
(j) $2x^4 + 3x^3 + 6x^2 + 11x - 10$.

2. Show that the ordinates of the maximum and minimum points of

$$y = f(x) = x^3 + 3Hx + G$$

(if there are any) are

$$y_1 = 2H\sqrt{-H} + G, \qquad y_2 = -2H\sqrt{-H} + G.$$

Let $\Delta = G^2 + 4H^3$. Observing that $\Delta = y_1 y_2$, prove that $f(x)$ has

(a) exactly one real root if $\Delta > 0$.
(b) three real roots if $\Delta < 0$.
(c) at least two equal roots if $\Delta = 0$. (Compare with Ex. 4 (b), p. 50.)

3. Determine all values of a for which the equation

$$x^3 + ax + a + 1 = 0$$

has a double root.

4. Show that if c is any real number the equation

$$2x^3 + 3x^2 + 6x + c = 0$$

has only one real root.

36. Isolation of the real roots of an equation with real coefficients. The real roots of an equation are said to have been *isolated* if one or more intervals have been found such that each real root is contained in one of these intervals and each interval contains only one root. For example, the roots of the equation

$$3x^4 - 2x^3 - 36x^2 + 36x - 8 = 0$$

were isolated in § 31. It was found that each of the intervals $[-4, -3]$, $[0, \frac{1}{2}]$, $[\frac{1}{2}, 1]$, $[3, 4]$ includes one and only one root of this equation, and all the roots are accounted for. The method there employed is clearly not applicable to all polynomials.

The first complete solution of the problem of isolating the real roots of an equation with real coefficients was furnished in 1829 by Sturm, whose solution will now be described.

Let $f_0(x), f_1(x), \cdots, f_r(x)$ be an ordered set of polynomials in the field of real numbers. Substituting $x = a$ (a real number), an ordered set of real numbers $f_0(a), f_1(a), \cdots, f_r(a)$ is obtained. All zeros present in this set are suppressed, except $f_0(a)$ and $f_r(a)$ if either or both of these numbers are 0, and the number of *variations in sign* in passing from term to term of the modified sequence is counted, this number being denoted by V_a. For example, the number of variations in sign of the sequence

$$4, 9, 0, -2, -1, 0, 0, 3, -5, 8$$

is 4. Special provision must be made for counting the number of variations in sign when $f_0(a)f_r(a) = 0$.

The basic idea of Sturm's method is to construct, corresponding to any given polynomial with real coefficients, a sequence of polynomials of which it may be asserted that, for any a and any b $(a < b)$, $V_a - V_b$ is the *exact number* of real roots between a and b of the given polynomial.

The polynomials which Sturm proved to have the desired prop-

erty are constructed in the following manner: If $f(x)$ is the given polynomial, let $f_0(x) = f(x)$ and $f_1(x) = f'(x)$. On dividing $f_0(x)$ by $f_1(x)$ a remainder is obtained, whose *negative* is $f_2(x)$. The negative of the remainder obtained when $f_1(x)$ is divided by $f_2(x)$ is $f_3(x)$; etc. The polynomials $f_0(x), f_1(x), f_2(x), \cdots$ thus obtained are called the *Sturm functions* for the given polynomial $f(x)$. The method of calculating the Sturm functions for $f(x)$ is similar to the Euclidean algorithm for the polynomials $f(x)$ and $f'(x)$, the difference being that the sign of each remainder is changed before proceeding to the next division. The calculations terminate naturally when a remainder is obtained which is a constant, whose negative is the last Sturm function. It is, however, permissible to stop with any Sturm function which does not change sign in the interval $[a, b]$ under consideration. As we are usually concerned with the isolation of all the real roots, we stop with any Sturm function which *never changes sign*. The process may be modified, where convenient, by multiplying any Sturm function by a *positive* number before proceeding to the next division. These modified functions are also called Sturm functions for the given polynomial.

Example. Isolate the real roots of

$$f(x) = 2x^4 - 14x^2 + 14x - 1.$$

A table of values is first constructed, as it may give all the information desired, and in any case provides bounds for the real roots. Omitting details, which the student should work out for himself, we find:

x	-4	-3	-2	-1	0	1	2	3
$f(x)$	231	-7	-53	-27	-1	1	3	77

The table of values shows that each of the intervals $[-4, -3]$, $[0, 1]$ contains one or three roots of $f(x)$ but provides no further information concerning the problem of isolating the roots. In some problems similar to the one under consideration the existence of imaginary roots of $f(x)$ may be demonstrated by showing that one of the derivatives of $f(x)$ has imaginary roots, but no such short-cut to the solution of the present problem is available.

The Sturm functions are now calculated and the following table constructed:

x	$-\infty$	0	∞	1	2
$f_0(x) = 2x^4 - 14x^2 + 14x - 1$	+	−	+	+	+
$f_1(x) = 4x^3 - 14x + 7$	−	+	+	−	+
$f_2(x) = 14x^2 - 21x + 2$	+	+	+	−	+
$f_3(x) = 39x - 43$	−	−	+	−	+
$f_4(x) = +$	+	+	+	+	+
V_x	4	3	0	2	0

Here $f_1(x) = \frac{1}{2}f'(x)$. Before dividing $f_0(x)$ by $f_1(x)$, $f_0(x)$ is multiplied by 2 to avoid fractions. The negative of the remainder of this division is $f_2(x)$, a polynomial of degree 2. Had its discriminant been negative the division process would have terminated at this point. In the present example the division process must be continued. Only the sign of $f_4(x)$ has been indicated as its actual value is immaterial.

We first find $V_{-\infty}$, V_0 and V_∞ as no computations are necessary. Sturm's Theorem assures us that, since $V_{-\infty} - V_0 = 1$ and $V_0 - V_\infty = 3$, $f(x)$ has exactly one negative root (now isolated with the aid of our table of values) and exactly three positive roots. The last two columns of the table are constructed for the purpose of isolating the three positive roots. Since $V_0 - V_1 = 1$, the interval $[0, 1]$ contains exactly one root. Since $V_1 - V_2 = 2$, the interval $[1, 2]$ contains exactly two roots. We find that $f(\frac{3}{2})$ is negative and conclude that $f(x)$ has four real roots, one in each of the intervals $[-4, -3]$, $[0, 1]$, $[1, \frac{3}{2}]$, $[\frac{3}{2}, 2]$.

37. Sturm's Theorem. Let $f_0(x) = f(x)$ be a polynomial of degree ≥ 1 with real coefficients and having no multiple roots so that $f(x)$ and $f_1(x) = f'(x)$ are relatively prime. The Euclidean algorithm for the polynomials $f_0(x)$ and $f_1(x)$ is modified by changing the sign of each remainder before proceeding to the next division, yielding the following equations:

$$\begin{aligned} f_0(x) &= q_1(x)f_1(x) - f_2(x), \\ f_1(x) &= q_2(x)f_2(x) - f_3(x), \\ &\cdots\cdots \\ f_{k-2}(x) &= q_{k-1}(x)f_{k-1}(x) - f_k(x), \end{aligned}$$

the last remainder being either a constant or a polynomial which never changes sign. If $f_k(x)$ is a constant it cannot be 0 since $f_0(x)$ and $f_1(x)$ are relatively prime.

THEOREM 6. (STURM.) *For a real number x let V_x be the number of variations in sign of the Sturm functions $f_0(x), f_1(x), \cdots, f_k(x)$*

for the polynomial $f(x)$. *If* a *and* b *are real numbers* $(a < b)$, *then* $V_a - V_b$ *is the exact number of roots of* $f(x)$ *in the interval* $[a, b]$ *if* $f(a)f(b) \neq 0$.

Let $[\alpha, \beta]$ be an interval which includes at most one root of

$$f_0(x)f_1(x) \cdots f_k(x) = 0.$$

The root in question may be α or β; only the case $f(\alpha)f(\beta) = 0$ is excluded. We proceed to determine the value of $V_\alpha - V_\beta$. The following cases arise.

1. The interval $[\alpha, \beta]$ contains no root of any of the Sturm functions. Since none of these functions changes sign in the interval, $V_\alpha - V_\beta = 0$.

2. The function $f_r(x)$, $(0 < r < k)$, and no other Sturm function, has a root in the interval. This function has a predecessor $f_{r-1}(x)$ and a successor $f_{r+1}(x)$ connected by the relation

$$f_{r-1}(x) = q_r(x)f_r(x) - f_{r+1}(x).$$

Hence, if ρ is the root of $f_r(x)$ in the interval $[\alpha, \beta]$,

$$f_{r-1}(\rho) = -f_{r+1}(\rho) \neq 0.$$

The signs of $f_{r-1}(x)$ *and* $f_{r+1}(x)$ *are therefore opposite throughout the interval* $[\alpha, \beta]$. An exhaustive enumeration of the various possible combinations of signs of $f_{r-1}(x)$, $f_r(x)$, and $f_{r+1}(x)$, including the cases in which $\rho = \alpha$ or β, is given by the following table:

x	$\alpha\ \beta$	$\alpha\ \beta$	$\alpha\ \beta$	$\alpha\ \beta$	$\alpha\ \beta$	$\alpha\ \beta$	$\alpha\ \beta$	$\alpha\ \beta$	$\alpha\ \beta$	$\alpha\ \beta$	$\alpha\ \beta$	$\alpha\ \beta$
$f_{r-1}(x)$	+ +	− −	+ +	− −	+ +	− −	+ +	− −	+ +	− −	+ +	− −
$f_r(x)$	− +	− +	+ −	+ −	0 +	0 +	0 −	0 −	+ 0	+ 0	− 0	− 0
$f_{r+1}(x)$	− −	+ +	− −	+ +	− −	+ +	− −	+ +	− −	+ +	− −	+ +

The table shows that in each of the cases which may arise $V_\alpha - V_\beta = 0$ as far as these three functions are concerned. Since none of the other Sturm functions changes sign in the interval, $V_\alpha - V_\beta = 0$ for the entire set of functions.

3. The function $f_k(x)$, and no other Sturm function, has a root in the interval. As this function never changes sign, $f_k(\alpha)$ and $f_k(\beta)$ have the same sign if neither vanishes. Therefore no Sturm function changes sign in the interval, and $V_\alpha - V_\beta = 0$.

If $f_k(\alpha) = 0$ or $f_k(\beta) = 0$, the 0 may not be omitted in computing V_α or V_β as the case may be. By agreeing to give $f_k(\alpha)$ and $f_k(\beta)$

(if either vanishes) the sign which $f_k(x)$ has when it does not vanish, we again have $V_\alpha - V_\beta = 0$.

4. The function $f_0(x) = f(x)$ has a root $x = \rho$ *within* the interval $[\alpha, \beta]$, and ρ is not a root of any other Sturm function. Since $f'(\rho)$ is positive or negative according as $f(x)$ is increasing or decreasing at $x = \rho$, only two cases arise:

$$\begin{array}{lcccc} & \alpha & \beta & \alpha & \beta \\ f_0(x) & - & + & + & - \\ f_1(x) & + & + & & \end{array}$$

Since no Sturm function, except $f_0(x)$, changes sign in the interval, it follows that $V_\alpha - V_\beta = 1$. Of the cases considered this is the first in which $V_\alpha - V_\beta > 0$.

5. Two or more Sturm functions have the same root ρ in the interval. No two of these functions are *successive* functions. For if ρ is a common root of $f_r(x)$ and $f_{r+1}(x)$, then ρ is a root of $f_{r-1}(x)$ since

$$f_{r-1}(x) = q_r(x)f_r(x) - f_{r+1}(x).$$

Again, from the relation

$$f_{r-2}(x) = q_{r-1}(x)f_{r-1}(x) - f_r(x),$$

we have $f_{r-2}(\rho) = 0$; etc. It follows that ρ is a common root of $f(x)$ and $f'(x)$, whereas these polynomials are relatively prime.

Applying the results of the first four cases to each of the Sturm functions which have ρ as a root we conclude that $V_\alpha - V_\beta = 1$ *if a root of* $f(x)$ *is within the interval* $[\alpha, \beta]$ *and is* 0 *otherwise.*

We now consider any interval $[a, b]$, subject only to the restriction that $f(a)f(b) \neq 0$. This interval is divided into a finite number of subintervals

$$[a_1, a_2], [a_2, a_3], \cdots, [a_{m-1}, a_m], \qquad (a = a_1, b = a_m),$$

each of which contains at most one root of the equation

$$f_0(x)f_1(x) \cdots f_k(x) = 0,$$

while no root of $f(x)$ occurs at either end of any subinterval. We have

$$V_a - V_b = (V_{a_1} - V_{a_2}) + (V_{a_2} - V_{a_3}) + \cdots + (V_{a_{m-1}} - V_{a_m}).$$

Each of the terms in parentheses of the right member has the value 1 or 0 according as $f(x)$ does or does not have a root in the

corresponding subinterval. Therefore $V_a - V_b$ *is the exact number of roots of* $f(x)$ *in the interval* $[a, b]$.

In the course of the proof of Sturm's Theorem we have seen that a term which vanishes may be omitted in computing V_a or V_b if it does not occur at the beginning or the end of the sequence. A zero occurring at the end may not be ignored but is to be replaced by that sign which the last Sturm function has for all values for which it does not vanish. The case in which the first Sturm function $f(x)$ vanishes at the beginning or at the end of the interval is avoided in practice.

We assumed that $f(x)$ had no multiple roots. By a modification of the argument it may be shown that Sturm's Theorem is valid even if $f(x)$ has multiple roots, provided that each multiple root is counted only once.

EXERCISES

1. Prove that if any Sturm function is multiplied by a positive number before proceeding to the next division, the modified set of functions also has the property expressed by Sturm's Theorem.

2. Isolate the real roots of the following equations:

(a) $x^4 - 2x^2 + 12x - 18 = 0$. *Ans.* $[-3, -2], [1, 2]$.

(b) $x^4 - 4x + 6 = 0$. *Ans.* No real roots.

(c) $24x^4 - 24x^2 + 3x + 4 = 0$.

(d) $x^4 + 4x^3 - 6x + 2 = 0$.

(e) $x^4 + 4x^3 + x^2 - 6x + 2 = 0$.

Ans. $[-3, -\frac{5}{2}], [-\frac{5}{2}, -2], [0, \frac{1}{2}], [\frac{1}{2}, 1]$.

(f) $x^4 + 4\sqrt{3}x^3 + 2\sqrt{3}x^2 + 4x + 1 = 0$.

(g) $x^5 - 2x^2 - 3x - 2 = 0$.

(h) $x^6 - 3x^4 + 3x^2 + 6x - 1 = 0$.

(i) $x^6 + x + 1 = 0$.

(j) $x^4 + 4x^3 - 6x^2 - 4x - 1 = 0$.

(k) $2x^4 - 16x^3 + 20x^2 - 8x + 1 = 0$.

Ans. $[0, .3], [.3, .5], [.5, 1], [6, 7]$.

3. Show without using Sturm's Theorem that the equation

$$x^4 - x^3 + ax^2 + x + 1 = 0 \qquad (a \geq 2)$$

has no real root. [Write the equation in the form

$$x^2(x^2 - x + 1) + (a - 1)x^2 + x + 1.]$$

4. Show similarly that none of the following equations has a real root:

(a) $x^4 - 2x^3 + 3x^2 + x + 5 = 0$.

(b) $2x^6 - 3x^5 + 2x^4 + x^2 + 1 = 0$.

(c) $3x^6 + x^5 + 3x^4 - 2x^3 + 5x^2 - x + 3 = 0$.

38. Budan's Theorem. The successive derivatives of a polynomial are so easily calculated that it is only natural to inquire whether $V_a - V_b$ for the functions

$$(1) \qquad f(x), f'(x), f''(x), \cdots, f^{(k)}(x)$$

gives any information at all concerning the number of roots of $f(x)$ in the interval $[a, b]$. There is, however, no need of restricting our investigation to polynomials since the sequence (1) is defined for a much wider class of functions.

A function $f(x)$ is *analytic* at $x = c$ if the Taylor series

$$(2) \qquad f(x) = f(c) + (x - c)f'(c) + (x - c)^2 \frac{f''(c)}{2!} +$$

converges for every x in an interval which includes c and at least one other number. If $f(x)$ is analytic at $x = c$ there exists a positive number R (R may be infinite) such that (2) converges for every x within the interval $[c - R, c + R]$. If $f(x)$ is analytic at $x = c$, $f(x)$ is also analytic at $x = a$, where a is any number within the interval of convergence. An analytic function is continuous within the interval of convergence and possesses continuous derivatives of all orders within this interval.* If, in (2),

$$f(c) = 0, f'(c) = 0, \cdots, f^{(m-1)}(c) = 0, f^{(m)}(c) \neq 0,$$

the series begins with $(x - c)^m$ and c is a root of multiplicity m of $f(x)$.

THEOREM 7. (BUDAN.) *Let $f(x)$ be a function which is analytic in the interval $[a, b]$, does not vanish at either end of the interval, and whose kth derivative has no root in the interval. For a real x let V_x denote the number of variations in sign of the sequence* (1). *The number of roots of $f(x)$ in the interval $[a, b]$ is $V_a - V_b - e$, where e is an even number ≥ 0. A root of multiplicity m is counted as m roots.*

If $f(x)$ is a polynomial of degree n, the condition that $f^{(k)}(x)$ have no root in the interval is satisfied when $k = n$ but may be satisfied by a smaller value. On the other hand, if $f(x)$ is a transcendental function no finite number k may exist for which this condition is satisfied. In such cases Theorem 7 is inapplicable. For example, each of the successive derivatives of $f(x) = \cos x$ has a root in the interval $[0, 2\pi]$.

* For proofs the reader is referred to textbooks in Analysis.

Let $[\alpha, \beta]$ be a subinterval of $[a, b]$ which includes at most one root of the equation

$$f(x)f'(x)f''(x) \cdots f^{(k)}(x) = 0 \tag{3}$$

and such that $f(\alpha)f(\beta) \neq 0$. The following cases arise.

1. The interval $[\alpha, \beta]$ includes no root of (**3**). Clearly $V_\alpha - V_\beta = 0$.

2. $f^{(r)}(x), f^{(r+1)}(x), \cdots, f^{(r+s-1)}(x), \ (0 < r \leq r + s - 1 < k)$ have a common root $x = \rho$ in the interval,* which is not a root of any other function of the set (**1**). Suppose $\rho \neq \alpha$ or β and $f^{(r+s)}(\rho) > 0$. Since $f^{(r+s)}(x)$ is positive throughout the interval $[\alpha, \beta]$, $f^{(r+s-1)}(x)$ increases as x increases from $x = \alpha$ to $x = \beta$; hence $f^{(r+s-1)}(\alpha) < 0$ and $f^{(r+s-1)}(\beta) > 0$. Therefore, if $s > 1$, $f^{(r+s-2)}(x)$ decreases in the interval $[\alpha, \rho]$, vanishes at ρ, and increases in the interval $[\rho, \beta]$; hence this function is positive throughout the interval $[\alpha, \beta]$, except at ρ. Repeated applications of the preceding argument yield finally the following table of signs:

	$f^{(r-1)}(x)$	$f^{(r)}(x)$	$f^{(r+1)}(x)$	$\cdots$	$f^{(r+s-2)}(x)$	$f^{(r+s-1)}(x)$	$f^{(r+s)}(x)$
α		$(-1)^s$	$(-1)^{s-1}$	$\cdots$	$+$	$-$	$+$
β		$+$	$+$	$\cdots$	$+$	$+$	$+$

The signs of $f^{(r-1)}(\alpha)$ and $f^{(r-1)}(\beta)$ have been omitted; they are both positive or both negative. If s is even, $V_\alpha - V_\beta = s$. If s is odd, $V_\alpha - V_\beta = s + 1$ or $s - 1$ according as $f^{(r-1)}(x)$ is positive or negative in the interval $[\alpha, \beta]$. Therefore $V_\alpha - V_\beta$ is an *even* number ≥ 0.

The same result is obtained if $\rho = \alpha$ or β or if $f^{(r+s)}(\rho) < 0$.

3. The function $f(x)$ has a root $x = \rho$ of multiplicity s in the interval, while $f^{(j)}(\rho) \neq 0$ if $j \geq s$. By assumption $\rho \neq \alpha$ or β. A discussion similar to that of Case 2 leads to the conclusion that $V_\alpha - V_\beta = s$, as the function $f^{(r-1)}(x)$ does not occur in the present case.

4. Two or more of the functions (**1**) have the same root ρ in the interval. These may be grouped into sets of *successive* functions which have ρ as a root. From the results of the preceding cases we conclude that $V_\alpha - V_\beta$ is an even number ≥ 0 if ρ is not a root of $f(x)$ and equals $s +$ an even number ≥ 0 if ρ is a root of multiplicity s of $f(x)$.

* By assumption, $f^{(k)}(x)$ does not vanish in the interval; hence $r + s - 1 < k$. If $s = 1$, only one function, $f^{(r)}(x)$, has ρ as a root.

By hypothesis $[a, b]$ is an interval in which $f^{(k)}(x)$ does not vanish and at whose ends $f(x)$ does not vanish. This interval is divided into subintervals

$$[a_1, a_2], [a_2, a_3], \quad , [a_{m-1}, a_m], \qquad (a_1 = a, a_m = b),$$

each of which includes at most one root of (3), no root of $f(x)$ occurring at the beginning or at the end of any subinterval. We have

$$V_a - V_b = (V_{a_1} - V_{a_2}) + (V_{a_2} - V_{a_3}) + \cdots + (V_{a_{m-1}} - V_{a_m}).$$

If $[a_{i-1}, a_i]$ does not include a root of $f(x)$, $V_{a_{i-1}} - V_{a_i}$ is an even number ≥ 0. If this subinterval includes a root of $f(x)$ of multiplicity s, $V_{a_{i-1}} - V_{a_i} = s +$ an even number ≥ 0. Therefore, if exactly N roots of $f(x)$ are contained in the interval $[a, b]$, $V_a - V_b = N + e$, as asserted by Budan's Theorem.

Example. Isolate the real roots of the equation

$$f(x) = e^x + 5x^2 - 7x = 0.$$

The table

x	$-\infty$	0	∞	1
$f(x) = e^x + 5x^2 - 7x$	$+$	$+$	$+$	$+$
$f'(x) = e^x + 10x - 7$	$-$	$-$	$+$	$+$
$f''(x) = e^x + 10$	$+$	$+$	$+$	$+$
V_x	2	2	0	0

shows that there are no negative roots and either two or no positive roots. We stopped with $f''(x)$ because this function vanishes for no real x. If $f(x)$ has two positive roots they must be in the interval $[0, 1]$ since $V_0 - V_1 = 2$. We find that $f(\frac{1}{2})$ is negative and conclude that the proposed equation has exactly two real roots, one in each of the intervals $[0, \frac{1}{2}]$, $[\frac{1}{2}, 1]$.

39. Descartes' Rule of Signs. Budan's Theorem, applied to the interval $[0, \infty]$, yields the

THEOREM 8. (DESCARTES' RULE OF SIGNS.) *Let*

$$f(x) = c_0 + c_1x + c_2x^2 + \cdots$$

be a polynomial or a power series which converges for every x and whose coefficients involve only a finite number of variations in sign.

The number of positive roots of $f(x)$ equals the number of variations in sign of the coefficients of $f(x)$ minus an even number ≥ 0.

If $c_0 = 0$, a power of x may be removed from $f(x)$ and Descartes' Rule then applied. We suppose hereafter that $c_0 \neq 0$.

By assumption, if $f(x)$ is an infinite series, an integer n exists such that the sequence

$$c_n, c_{n+1}, \cdots \qquad (c_n \neq 0)$$

has no variations in sign. If $f(x)$ is a polynomial we suppose its degree to be n. In either case $f^{(n)}(x)$ has no positive root since all its coefficients have the same sign. Therefore, by Budan's Theorem, the number of positive roots of $f(x)$ is

$$N = V_0 - V_\infty - e, \tag{1}$$

where e is an even number ≥ 0, and V_x is the number of variations in sign of

$$f(x), f'(x), \cdots, f^{(n)}(x). \tag{2}$$

If $f(x)$ is a polynomial, it follows from Theorem 3 that $V_\infty = 0$; for the sign of each of the functions (**2**), for sufficiently large values of x, is that of the leading coefficient c_n of $f(x)$. If $f(x)$ is an infinite series, the sign of the polynomial

$$c_0 + c_1x + \cdots + c_nx^n,$$

and the sign of each of the first n derivatives of this polynomial is, for x sufficiently large, the sign of c_n. The sign of the power series

$$c_{n+1}x^n + c_{n+2}x^{n+2} + \cdots,$$

and the sign of each of the derivatives of this series is, for every positive x, the sign of c_n. Therefore the sign of each of the functions (**2**), for all sufficiently large values of x, is that of c_n. Hence $V_\infty = 0$. Therefore, by (**1**),

$$N = V_0 - e.$$

The theorem now follows from the observation that, since $c_0 = f(0)$, and

$$c_k = f^{(k)}(0)/k!, \qquad (k = 1, \cdots)$$

V_0 is the number of variations in sign of $c_0, c_1, \cdots, c_n$.

The preceding argument breaks down if $f(x)$ has a finite interval

of convergence $[-R, R]$, since the series does not represent $f(x)$ for $|x| > R$. In this case let $\epsilon > 0$ be chosen so small that all the roots of $f(x)$ within the interval $[0, R]$ are within the interval $[0, R - \epsilon]$. Such an ϵ exists if the coefficients of $f(x)$ involve only a finite number of variations in sign, as assumed.* For $f^{(n)}(x)$ has no positive root within the interval of convergence, n being some positive integer. Therefore, by Rolle's Theorem, $f(x)$ has only a finite number of positive roots within the interval of convergence.

The number of roots of $f(x)$ in the interval $[0, R - \epsilon]$ is, by Budan's Theorem

$$N = V_0 - V_{R-\epsilon} - e.$$

Therefore $N \leq V_0$. But we cannot conclude that $V_0 - N$ is an *even* number.

THEOREM 9. *The number of positive roots within the interval of convergence of a power series*

$$c_0 + c_1x + c_2x^2 + \cdots$$

is not greater than the number of variations in sign of its coefficients.

The preceding theorems, applied to the function $f(-x)$, may give information concerning the negative roots of $f(x)$.

EXERCISES

1. Find limits for the number of positive and the number of negative roots of

(a) $3x^4 - x^3 - 5x^2 - 1 = 0.$
(b) $x^6 + 4x^2 + 1 = 0.$
(c) $x^5 + 2x^3 + 8x - 1 = 0.$
(d) $x^6 + x - 1 = 0.$
(e) $x^6 - x + 1 = 0.$
(f) $x^6 - x^2 + x + 2 = 0.$
(g) $x^7 - 2x^5 - 7x^3 + x^2 - 9x + 6 = 0.$
(h) $2x^4 + 6x^3 + x^2 + 8x + 5 = 0.$

2. Find the interval of convergence of each of the following power series and apply Theorem 8 or Theorem 9.

(a) $-1 - x + \dfrac{x^2}{2!} + \dfrac{x^3}{3!} + \cdots.$

(b) $2 - x + \dfrac{x^3}{3!} + \dfrac{x^5}{5!} + \cdots.$

* In the contrary case it may happen that no such ϵ exists. For example, the power series for $\sin 1/(1 - x)$ converges for $-1 < x < 1$ but has an infinite number of roots near 1, namely $1 - 1/k\pi$, where k is a positive integer.

(c) $1 + x - x^2 + x^3 + x^4 + x^5 +$

(d) $2x \quad \frac{x^2}{2} - \frac{x^3}{3} - \frac{x^5}{5} - \cdots.$

3. Isolate the real roots of the following equations.

(a) $x^4 + 2x^3 + 6x^2 - 6x + 1 = 0.$

(b) $x^4 + x^3 - 3x^2 - 2x + 2 = 0.$

(c) $x^6 + x^5 + x^4 + x^3 + x^2 - 4x + 1 = 0.$ [The second derivative equals $2\{x^2(15x^2 + 10x + 3) + (3x^2 + 3x + 1)\}$ and is therefore always positive.] *Ans.* $[0, \frac{1}{2}]$, $[\frac{1}{2}, 1]$.

(d) $x^6 - 2x^4 + 5x^2 + 7x + 1 = 0.$

(e) $x^7 - 3x^6 + 4x^5 + x^3 + 2x + 1 = 0.$ *Ans.* $[-1, 0]$.

(f) $x^8 - x^6 + x^4 - 7x + 4 = 0.$ *Ans.* $[0, 1]$, $[1, 2]$.

4. Isolate the real roots of the following equations.

(a) $\sin x - x^2 - 3x + 5 = 0.$

(b) $\sin x - \cos x + 2x^2 - 3 = 0.$

(c) $\log_{10} x + x^2 + 1 = 0.$ *Ans.* $[.01, 1]$.

40. Horner's method. Horner's method of calculating the real roots of a polynomial with real coefficients to any desired degree of accuracy is best explained with the aid of an illustrative example.

Example. Find the real roots of the equation

$$x^3 - 7x + 7 = 0. \tag{1}$$

There are three real roots, one in each of the intervals $[-4, -3]$, $[1, \frac{3}{2}]$, $[\frac{3}{2}, 2]$. We shall illustrate Horner's method by calculating the largest of these roots.

The roots of the equation are first diminished by 1 in order to bring the desired root in the interval $[0, 1]$. The equation

$$x^3 + 3x^2 - 4x + 1 = 0 \tag{2}$$

is obtained. The root of this equation which corresponds to the desired root of (**1**) lies in the interval $[\frac{1}{2}, 1]$. By trial we find this root to be in the smaller interval $[.6, .7]$. The corresponding root of (**1**) is in the interval $[1.6, 1.7]$. Diminishing the roots of (**2**) by .6, the equation

$$x^3 + 4.8x^2 + .68x - .104 = 0 \tag{3}$$

is obtained, which has a root in the interval $[0, .1]$. An approximate value of this root is obtained by solving the linear equation

$$.68x - .104 = 0,$$

whose root is $x = .1+$. We infer that the root of (**3**) in the interval $[0, .1]$ is near .1. We find by trial that the root lies between .09 and .1. The corresponding root of (**1**) lies between 1.69 and 1.70.

Diminishing the roots of (**3**) by .09, the equation

$$x^3 + 5.07x^2 + 1.5683x - .003191 = 0 \tag{4}$$

is obtained. Ignoring the first two terms of this equation we find that $x = .002+$. The root of (**4**) in the interval $[0, .01]$ is in the narrower interval $[.002, .003]$, and the corresponding root of (**1**) is in the interval $[1.692, 1.693]$. Diminishing the roots of (**4**) by .002, the equation

$$x^3 + 5.076x^2 + 1.588592x - .000034112 = 0 \tag{5}$$

is obtained. The root of the equation

$$1.588592x - .000034112 = 0.$$

is $x = .00002147$. The division was carried out to four significant

1	1	0	−7	+7
		1	−6	**1**
		2	**−4**	
	1	**3**		
.6	1	3	−4	1
		.6	2.16	−1.104
		3.6	−1.84	− **.104**
		.6	2.52	
		4.2	**.68**	
		.6		
	1	**4.8**		
.09	1	4.8	.68	− .104
		.09	.4401	.100809
		4.89	1.1201	− **.003191**
		.09	.4482	
		4.98	**1.5683**	
		.09		
	1	**5.07**		
.002	1	5.07	1.5683	− .003191
		.002	.010144	.003156888
		5.072	1.578444	− **.000034112**
		.002	.010148	
		5.074	**1.588592**	
		.002		
	1	**5.076**		

figures because four zeros appeared after the decimal point. In justification of this operation we remark that if we substitute this value of x in (5) the first two terms will not affect the seventh decimal place. The required root is therefore 1.6920215, to seven decimal places.

The successive transformations are conveniently effected by synthetic division, the work being arranged as shown on page 92.

EXERCISES

1. Find the irrational real roots of the following equations correct to five decimal places.

(a) $2x^3 + 3x^2 + 6x - 12 = 0.$ *Ans.* 1.05408.

(b) $x^3 - 3x + 1 = 0.$ *Ans.* .34730, 1.53206, −1.87938.

(c) $x^3 = 5.$

(d) $x^4 - 2x^2 + 12x - 18 = 0.$ (Ex. 2 (a), p. 85.) *Ans.* 1.47065, −2.88487.

2. Find cos 20° without consulting trigonometric tables. [Use the identity $\cos 3\theta = 4\cos^3\theta - 3\cos\theta$.]

3. A 3-gallon can is to be constructed so that its height exceeds its radius by 2 inches. Find the dimensions of the can. (1 gallon = 231 cubic inches.) *Ans.* $r = 5.444$ in.

4. Find the length of the edge of a cube which would be transformed into a rectangular box having twice the volume of the cube if the edges of the cube were increased by 1, 2, and 3 inches respectively.

5. Find the coordinates of the point on the parabola $y = x^2$ which is nearest the point (2, 1). *Ans.* (1.165, 1.357).

6. Find the coordinates of the points of intersection of the hyperbola $xy = 1$ and the circle $(x - 1)^2 + y^2 = 1$. *Ans.* (1, 1), (1.839, .5437).

41. Newton's method. If an approximation to a root of an equation $f(x) = 0$ has been obtained, a better approximation may be obtained by Newton's method, which will now be described. Before applying this method it must be verified that the equation has only one root within a certain interval $[a, b]$ so that $f(a)$ and $f(b)$ have opposite signs, and that neither $f'(x)$ nor $f''(x)$ vanishes in the interval. The following cases may then arise:

	$f(a)$	$f(b)$	$f'(x)$	$f''(x)$ $(a \leq x \leq b)$
1.	−	+	+	+
2.	−	+	+	−
3.	+	−	−	+
4.	+	−	−	−

These cases are illustrated graphically by the following figures.

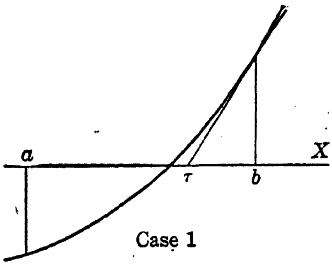

FIG. 8

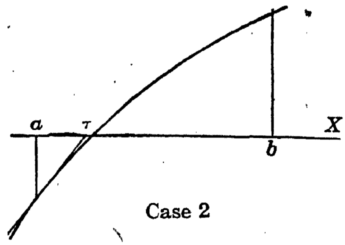

FIG. 9

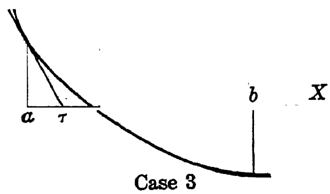

FIG. 10

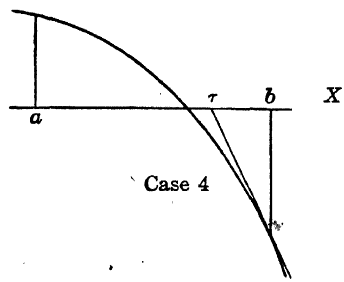

FIG. 11

The equation of the tangent line to the curve $y = f(x)$ at the point $(x_0, f(x_0))$ is

$$y - f(x_0) = f'(x_0)(x - x_0).$$

The x-axis intersects this line in a point whose abscissa is

$$\tau = x_0 - \frac{f(x_0)}{f'(x_0)}. \tag{1}$$

It is evident from the figures that if we choose $x_0 = b$ in Cases 1 and 4, then τ is nearer the root of $f(x) = 0$ in the interval $[a, b]$ than b; while if we choose $x_0 = a$ in Cases 2 and 3, then τ is nearer the root than a. Now in Cases 1 and 4 $f(b)$ and $f''(b)$ have the same sign, while in Cases 2 and 3 $f(a)$ and $f''(a)$ have the same sign. Hence: *If x_0 be chosen as that one of the two numbers a and b for which $f(x_0)$ and $f''(x_0)$ have the same sign, then τ (defined by* (**1**)*), is nearer the root than x_0.*

It is evident from the figures that $f(\tau)$ has the same sign as $f(x_0)$. Therefore (1) may be applied again, with x_0 replaced by τ, and a closer approximation to the root obtained. Repeated applications yield as close an approximation to the root as desired.*

Newton's method is applicable to transcendental equations and offers a material advantange over Horner's method in solving algebraic equations of high degree which involve a small number of terms.

Example 1. Find the root in the interval [1, 2] of the equation

$$f(x) = x^{10} - 10x + 4 = 0.$$

Before applying Newton's method, a smaller interval should be found which contains the root. We find by trial that the root lies in the interval [1.2, 1.3]. We have

$$f'(x) = 10(x^9 - 1), \qquad f''(x) = 90x^8.$$

For a closer approximation to the root use formula (1):

$$F(x) = x - \frac{f(x)}{f'(x)} = x - \frac{x^{10} - 10x + 4}{10(x^9 - 1)}.$$

Since $f''(x)$ is positive throughout the interval and $f(1.2) < 0$ while $f(1.3) > 0$, we choose $x = 1.3$. We find (using a table of logarithms to compute x^9 and x^{10})

$$\begin{aligned} F(1.3) &= \quad 1.3 - .04 &&= 1.26, \\ F(1.26) &= \quad 1.26 - .02 &&= 1.24, \\ F(1.24) &= \quad 1.24 - .0032 &&= 1.2368, \\ F(1.2368) &= 1.2368 - .000128 &&= 1.236672. \end{aligned}$$

Using a five-place table of logarithms, results cannot be expected to be accurate to more than five significant figures. Our answer is therefore 1.2367.

Since $f''(x) > 0$ in this example, each of the successive approximations should be taken too large rather than too small in order to keep $f(x)$ positive, so that the condition that $f(x)$ and $f''(x)$ have the same sign will be fulfilled before proceeding to the next approximation.

* The preceding discussion, appealing as it does to geometric intuition, does not constitute a rigorous proof of the validity of Newton's method. For an analytic proof the reader is referred to H. Weber, *Kleines Lehrbuch der Algebra* (1912), p. 163.

Example 2. Find the root in the interval [3, 4] of the equation

$$f(x) = \log_{10}(x^2 + 2) + x - 5 = 0.$$

The equation has a root in this interval; for

$$f(3) = \log 11 - 2 < 0, \qquad f(4) = \log 18 - 1 > 0.$$

With the aid of a table of common logarithms we find that the root is in the smaller interval [3.7, 3.8]. Differentiating, we have

$$f'(x) = \frac{2Mx}{x^2 + 2} + 1, \qquad f''(x) = \frac{2M(2 - x^2)}{(x^2 + 2)^2},$$

where $M = \log_{10}e = .43429$. Since $f(3.7) < 0$, $f(3.8) > 0$, and $f''(x)$ is negative in the interval, the successive approximations to the root are all to be less than the root. The formula for closer approximations to the root is

$$F(x) = x - \frac{f(x)}{f'(x)} = x - \frac{(x^2 + 2)[\log (x^2 + 2) + x - 5]}{x^2 + 2 + .86858x}.$$

We find that

$$F(3.7) = 3.7 + .08 = 3.78,$$
$$F(3.78) = 3.78 + .0068 = 3.7868.$$

The root is 3.7868.

EXERCISES

1. Show graphically that Newton's method may fail if $f'(x)$ or $f''(x)$ vanishes in the interval.

2. Find the root in the interval [1, 2] of the equation

$$x^{10} - 100x - 100 = 0. \qquad \textit{Ans. } 1.7539.$$

3. Find the real root of the equation

$$(x - 1)^9 + x^7 = 0.$$

4. Find the root in the interval [0, 1] of the equation

$$\log_{10} (x^2 + 1) + x - 1 = 0. \qquad \textit{Ans. } .78957.$$

5. Solve $e^x - 3x = 0$.

6. A chord of a circle cuts off one-eighth of the area of the circle. What central angle does it subtend? *Ans.* 1.7664 radians.

7. Find the length of the base of an isosceles triangle of area 1 inscribed in a circle of radius 2. *Ans.* .50192.

CHAPTER VI

ELIMINATION. RESULTANTS. SYMMETRIC FUNCTIONS

42. Introduction. It is often necessary to eliminate a variable x between two equations

$$(1) \qquad f(x) = 0, \qquad g(x) = 0,$$

involving x and one or more other variables $y, z, \cdots$. The general procedure is to combine these equations in such a way as to obtain from them an equation

$$(2) \qquad F(y, z, \cdots) = 0$$

which does not involve x. We then say that all sets of values $y, z, \cdots$ for which equations (**1**) have a common root must satisfy (**2**). But, unless the elimination has been performed properly, we cannot be sure of the converse: that, if $y, z, \cdots$ satisfy (**2**), then equations (**1**) have a common root.

Example. Eliminate x between the equations

$$(3) \qquad yx^2 - 2x + y = 0,$$

$$(4) \qquad x^2 + yx - 2 = 0.$$

Multiplying (**4**) by $-y$ and adding to (**3**), we obtain

$$-(2 + y^2)x + 3y = 0.$$

Solving this equation for x, substituting in (**3**), and simplifying, we obtain

$$(5) \qquad y^5 + 7y^3 - 8y = 0,$$

whose roots are

$$y = 0, \ \pm 1, \ \pm 2i\sqrt{2}.$$

But when we substitute $y = 0$ in (**3**) and (**4**) we obtain two equations which do *not* have a common root. Therefore (**5**) is not the true eliminant of (**3**) and (**4**).

This example illustrates the necessity of developing an adequate

theory of elimination. It is our intention to consider methods of obtaining an eliminant which furnishes a necessary and sufficient condition that two equations have a root in common.

43. Again the identity $A(x)G(x) + B(x)F(x) = 1$. Let

$$(1) \qquad A(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n$$

and

$$(2) \qquad B(x) = b_0x^m + b_1x^{m-1} + \cdots + b_{m-1}x + b_m$$

be two polynomials whose coefficients are independent variables. Since these polynomials are relatively prime, there exist a unique pair of polynomials

$$(3) \qquad F(x) = f_0x^{n-1} + f_1x^{n-2} + \cdots + f_{n-2}x + f_{n-1}$$

and

$$(4) \qquad G(x) = g_0x^{m-1} + g_1x^{m-2} + \qquad + g_{m-2}x + g_{m-1}$$

in the field $R(a_0, a_1, \cdots, a_n; b_0, b_1, \quad , b_m)$, such that

$$(5) \qquad A(x)G(x) + B(x)F(x) = 1.$$

The coefficients of $F(x)$ and $G(x)$ are rational functions of the a's and b's but need not be polynomials in these variables. If a polynomial $P = P(a_0, a_1, \cdots, a_n; b_0, b_1, \cdots, b_m)$ is a multiple of the denominators of the coefficients of $F(x)$ and $G(x)$, then

$$(6) \qquad F_1(x) = PF(x) \qquad \text{and} \qquad G_1(x) = PG(x)$$

are polynomials not only in x, but in the a's and b's; and

$$(7) \qquad A(x)G_1(x) + B(x)F_1(x) = P.$$

To find a polynomial P satisfying (7) let us calculate the coefficients of $F(x)$ and $G(x)$ by the method of undetermined coefficients as we did in Chapter II. We have by (5)

$$(8) \qquad \begin{aligned} &(a_0x^n + a_1x^{n-1} + \qquad + a_{n-1}x + a_n) \\ \times\ &(g_0x^{m-1} + g_1x^{m-2} + \qquad + g_{m-2}x + g_{m-1}) \\ +\ &(b_0x^m + b_1x^{m-1} + \qquad + b_{m-1}x + b_m) \\ \times\ &(f_0x^{n-1} + f_1x^{n-2} + \qquad + f_{n-2}x + f_{n-1}) = 1. \end{aligned}$$

Therefore

$$
(9)\quad \begin{array}{llr}
a_0g_0 & + b_0f_0 & = 0, \\
a_1g_0 + a_0g_1 & + b_1f_0 + b_0f_1 & = 0, \\
a_2g_0 + a_1g_1 + a_0g_2 & + b_2f_0 + b_1f_1 + b_0f_2 & = 0, \\
 & & \\
\qquad a_ng_m & \qquad + b_mf_{n-1} & = 1.
\end{array}
$$

This is a system of $m + n$ non-homogeneous linear equations in which the a's and b's are known and the f's and g's the unknowns. The coefficient determinant of (9), with rows and columns interchanged, is

$$
(10)\quad \rho(A, B) = \left|\begin{array}{cccccccc}
a_0 & a_1 & a_2 & \cdots & a_n & & & \\
 & a_0 & a_1 & a_2 & \cdots & a_n & & \\
 & & \cdot & \cdot & \cdot & \cdot & \cdot & \\
 & & & a_0 & a_1 & a_2 & \cdots & a_n \\
b_0 & b_1 & b_2 & \cdots & b_m & & & \\
 & b_0 & b_1 & b_2 & \cdots & b_m & & \\
 & & \cdot & \cdot & \cdot & \cdot & \cdot & \\
 & & & b_0 & b_1 & b_2 & \cdots & b_m
\end{array}\right| \begin{array}{l} \left.\vphantom{\begin{array}{c}a\\a\\a\\a\end{array}}\right\} m \text{ rows} \\ \left.\vphantom{\begin{array}{c}a\\a\\a\\a\end{array}}\right\} n \text{ rows} \end{array}
$$

The blank spaces of the determinant are to be filled with zeros. Since the system (9) is known to have a unique solution, $\rho(A, B) \neq 0$. Moreover, each of the unknowns is expressible as a fraction whose denominator is $\rho(A, B)$ and whose numerator is a determinant which equals a polynomial in the a's and b's, with integral coefficients. Therefore $\rho(A, B)$ will serve as the polynomial P previously referred to.

THEOREM 1. *If $A(x)$ and $B(x)$ are the polynomials* (**1**) *and* (**2**) *whose coefficients are independent variables, there exists a unique pair of polynomials $F_1(x)$ and $G_1(x)$, whose degrees are less than those of $A(x)$ and $B(x)$ respectively and whose coefficients are polynomials in the a's and b's with integral coefficients, such that*

$$A(x)G_1(x) + B(x)F_1(x) = \rho(A, B),$$

where $\rho(A, B)$ is the determinant (**10**).

The rule underlying the formation of the determinant (**10**) is quite simple and should be thoroughly understood. From the definition of "determinant" we have the

THEOREM 2. *$\rho(A, B)$ is a homogeneous polynomial with integral coefficients, of total degree $m + n$ in the variables $a_0, \cdots a_n, b_0,$*

$\cdots b_m$. *Each term of the expansion of* $\rho(A, B)$ *is the product of* m *of the* a*'s and* n *of the* b*'s.*

The determinant $\rho(B, A)$ may be obtained by mn successive interchanges of the rows of the determinant $\rho(A, B)$. Hence the

THEOREM 3. $\rho(B, A) = (-1)^{mn}\rho(A, B)$.

44. The resultant of two polynomials. With the notation of § 43, each of the equations

$$A(x)G(x) + B(x)F(x) = 1, \tag{1}$$

$$A(x)G_1(x) + B(x)F_1(x) = \rho(A, B) \tag{2}$$

is an identity in $x, a_0, \cdots, a_n, b_0, \cdots, b_m$. There is one important difference between these equations: $F_1(x)$ and $G_1(x)$ are polynomials in the a's and b's, while $F(x)$ and $G(x)$ are rational functions of the a's and b's. If particular values (elements of some field) are assigned to the a's and b's, it may happen that a denominator of one or more of the coefficients of $F(x)$ or $G(x)$ vanishes so that (**1**) ceases to be valid. But (**2**) remains valid no matter what values are assigned to the a's and b's. In particular (**2**) remains valid even if values are assigned to the a's and b's for which $A(x)$ and $B(x)$ become polynomials that are not relatively prime.

Suppose that for certain values of the a's and b's the polynomials $A(x)$ and $B(x)$ are not relatively prime. If, for these values, $\rho(A, B) \neq 0$, we may divide (**2**) by $\rho(A, B)$, thus inferring (**1**), from which it follows that $A(x)$ and $B(x)$ are relatively prime. This being contrary to supposition, we conclude that $\rho(A, B) = 0$.

Conversely, suppose that $\rho(A, B) = 0$ for certain values of the a's and b's. Then equations (**9**) of § 43 do not have a unique solution. Therefore (**1**) cannot be satisfied by polynomials $F(x)$ and $G(x)$ whose degrees are less than those of $A(x)$ and $B(x)$ respectively. We conclude that $A(x)$ and $B(x)$ are not relatively prime.

THEOREM 4. *A necessary and sufficient condition that the polynomials* $A(x)$ *and* $B(x)$ *have a common factor of degree* ≥ 1 *is that* $\rho(A, B) = 0$.

As a consequence $\rho(A, B) = 0$ is the true eliminant of the equations $A(x) = 0$ and $B(x) = 0$. $\rho(A, B)$ is called the *resultant* of the polynomials $A(x)$ and $B(x)$.

EXERCISES

1. Find the resultant of

(a) $a_0x + a_1$ and $b_0x + b_1$. *Ans.* $a_0b_1 - a_1b_0$.

(b) $a_0x^2 + a_1x + a_2$ and $b_0x^2 + b_1x + b_2$.

Ans. $a_0^2b_2^2 + a_0a_2b_1^2 - 2a_0a_2b_0b_2 - a_0a_1b_1b_2$
$+ a_1^2b_0b_2 - a_1a_2b_0b_1 + a_2^2b_0^2$.

(c) $a_0x^2 + a_1x + a_2$ and $b_0x + b_1$. *Ans.* $a_0b_1^2 - a_1b_0b_1 + a_2b_0^2$.

(d) a_0x^n and $b_0x^m + b_m$. *Ans.* $a_0^mb_m^n$.

2. Find all values of t for which the equations $tx^2 + (-t^2 - 1)x + 1 = 0$, $x^2 + (t^2 - t)x - 1 = 0$ have a common root; and find the common root in each case.

Ans. $t = 0,\ x = 1;\ t = 1,\ x = 1;\ t = -1,\ x = -1 \pm \sqrt{2}$.

3. Find all values of t for which the equations $x^3 - t = 0$, $x^2 + tx + t = 0$ have a common root; and find the common root in each case.

4. Solve the illustrative example of § 42.

5. Find the points of intersection of the circle

$$x^2 + y^2 + 4x - 2y + 3 = 0$$

and the hyperbola

$$x^2 + 4xy - y^2 + 10y - 9 = 0.$$

Ans. $(-1, 2)$, $(-3, 0)$, $(-2 \pm \frac{3}{5}\sqrt{5},\ 1 \pm \frac{1}{5}\sqrt{5})$.

6. Find the cartesian equation of the curve whose parametric equations are

(a) $x = t^2 - t + 1, \qquad y = 2t^2 + t - 3.$

Ans. $4x^2 - 4xy + y^2 - 23x + 7y + 19 = 0$.

(b) $x = \dfrac{2t + 1}{t^2 + 1}, \qquad y = \dfrac{t^2 + 2t - 1}{t^2 + 1}.$

45. Factored form of the resultant. Let

$$A(x) = a_0(x - x_1)(x - x_2) \cdots (x - x_n) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n, \tag{1}$$

$$B(x) = b_0(x - x_1')(x - x_2') \cdots (x - x_m') = b_0x^m + b_1x^{m-1} + \cdots + b_{m-1}x + b_m, \tag{2}$$

where $a_0, b_0, x_1, x_2, \cdots, x_n, x_1', x_2', \cdots x_m'$ are independent variables. We are dealing with the field $R(a_0, b_0, x_1, x_2, \cdots, x_n, x_1', x_2', \cdots, x_m')$ which includes the coefficients of $A(x)$ and $B(x)$ since (§ 18)

$$\begin{aligned} a_k &= (-1)^k a_0 \Sigma x_1x_2 \cdots x_k, \qquad (k = 1, 2, \cdots, n), \\ b_k &= (-1)^k b_0 \Sigma x_1'x_2' \cdots x_k', \qquad (k = 1, 2, \cdots, m). \end{aligned} \tag{3}$$

The equation

$$(4) \qquad A(x)G_1(x) + B(x)F_1(x) = \rho(A,\ B)$$

of § 43 is now to be thought of as an identity in the variables $a_0, b_0, x_1, \cdots, x_n, x_1', \cdots, x_m'$.

The polynomials $A(x)$ and $B(x)$ have a non-constant common factor if and only if one of the variables $x_1, \cdots, x_n$ equals one of the variables $x_1', \cdots, x_m'$. Therefore, by Theorem 4, $\rho(A,\ B)$ vanishes when $x_i = x_j'$. Consequently

$$(5) \qquad \rho(A,\ B) = k\Pi(x_i - x_j'),$$

where

$$(6) \qquad \begin{aligned} \Pi(x_i - x_j') = {} & (x_1 - x_1')(x_1 - x_2') \cdots (x_1 - x_m') \\ \times {} & (x_2 - x_1')(x_2 - x_2') \cdots (x_2 - x_m') \\ & \\ \times {} & (x_n - x_1')(x_n - x_2') \cdots (x_n - x_m') \end{aligned}$$

and k is a polynomial which is to be determined.

The first line of the right member of (6) equals $B(x_1)/b_0$ by (2); the second equals $B(x_2)/b_0$; etc. Hence

$$(7) \qquad \Pi(x_i - x_j') = \frac{1}{b_0{}^n} B(x_1)B(x_2) \cdots B(x_n).$$

The product of the factors in the first column of the right member of (6) equals $(-1)^n A(x_1')/a_0$ by (1); the product of the factors in the second column equals $(-1)^n A(x_2')/a_0$; etc. Hence

$$(8) \qquad \Pi(x_i - x_j') = \frac{(-1)^n}{a_0{}^m} \cdot A(x_1')A(x_2') \qquad A(x_m').$$

To determine the k in (5) we observe that, in view of (3), each term of the expansion of the determinant form of $\rho(A, B)$ is divisible by $a_0{}^m b_0{}^n$ and involves each x_i to at most the mth power and each x_j' to at most the nth power. By (6) $\Pi(x_i - x_j')$ is of degree m in each x_i and of degree n in each x_j'. Therefore

$$(9) \qquad \rho(A,\ B) = ca_0{}^m b_0{}^n \Pi(x_i - x_j'),$$

where c is a *numerical* constant. Consider the particular case

$$A(x) = x^n, \qquad B(x) = x^m + 1.$$

Since $x_1 = x_2 = \cdots = x_n = 0$, $\Pi(x_i - x_j') = 1$ by (7). Again

$$\rho(A, B) = \begin{array}{l} \left|\begin{array}{ccccccc} 1 & & & & & & \\ & 1 & & & & & \\ & & \cdots & & & & \\ & & & 1 & & & \\ & & & & 1 & & \\ & & & & & \cdot & \\ & & & & & & 1 \end{array}\right| \end{array} \begin{array}{l} \left.\vphantom{\begin{array}{c}1\\1\\1\\1\end{array}}\right\} m \text{ rows} \\ \left.\vphantom{\begin{array}{c}1\\1\\1\end{array}}\right\} n \text{ rows} \end{array} = 1.$$

It follows from (9) that $c = 1$.

THEOREM 5. *If $A(x)$ and $B(x)$ are defined by* (1) *and* (2) *respectively, then*

$$\text{(10)}\quad \rho(A, B) = a_0^m b_0^n \Pi(x_i - x_j') = a_0^m B(x_1) B(x_2) \cdots B(x_n)$$
$$= (-1)^{nm} b_0^n A(x_1') A(x_2') \cdots A(x_m').$$

The resultant of two polynomials may be calculated with the aid of (10) when all the roots of one of them are known.

46. Discriminant of a polynomial. On examining the first column of the determinant form of the resultant of

$$A(x) = a_0 x^n + \cdots + a_{n-1} x + a_n \qquad (n \geq 2)$$

and its derivative, it is evident that $\rho(A, A')$ has a_0 as a factor. Therefore $D(A)$, defined by

$$\text{(1)} \qquad \rho(A, A') = (-1)^{\frac{1}{2}n(n-1)} a_0 D(A),$$

is a polynomial in $a_0, a_1, \cdots, a_n$ with integral coefficients. It is called the *discriminant* of $A(x)$.

We have seen (§ 19) that $A(x)$ has a repeated factor if, and only if, $A(x)$ and $A'(x)$ have a common factor of degree ≥ 1. On the other hand, $A(x)$ and $A'(x)$ have a common factor of degree ≥ 1 if, and only if, $\rho(A, A') = 0$. Combining these results with (1), we have the following theorem.

THEOREM 6. *A necessary and sufficient condition that a polynomial have a repeated factor is that its discriminant vanish.*

We now suppose $A(x)$ to be expressed in the form

$$A(x) = a_0(x - x_1)(x - x_2) \cdots (x - x_n).$$

Then

$$
\begin{aligned}
A'(x_1) &= a_0(x_1 - x_2)(x_1 - x_3) \qquad (x_1 - x_n),\\
A'(x_2) &= a_0(x_2 - x_1)(x_2 - x_3) \qquad (x_2 - x_n),
\end{aligned}
$$

(2)

$$A'(x_n) = a_0(x_n - x_1)(x_n - x_2) \cdot \cdot \quad (x_n - x_{n-1}).$$

Multiplying, we have

(3) $$A'(x_1)A'(x_2) \cdots A'(x_n) = (-1)^{\frac{1}{2}n(n-1)}a_0{}^n \prod_{\substack{i,j=1\\ i>j}} (x_i - x_j)^2.$$

By Theorem 5, with $B(x) = A'(x)$, $m = n - 1$, we have

$$
\begin{aligned}
\rho(A, A') &= a_0{}^{n-1}A'(x_1)A'(x_2) \cdots A'(x_n)\\
&= (-1)^{\frac{1}{2}n(n-1)}a_0{}^{2n-1} \prod_{i>j} (x_i - x_j)^2.
\end{aligned}
$$

Comparing with (1), we conclude that

(4) $$D(A) = a_0{}^{2n-2} \prod_{i>j} (x_i - x_j)^2.$$

This expression for $D(A)$ in terms of the roots of $A(x)$ shows that $D(A) = 0$ if, and only if, at least two roots of $A(x)$ are equal, confirming Theorem 6.

EXERCISES

1. Find the resultant of

(a) $\dfrac{x^5 - 1}{x - 1}$ and $\dfrac{x^7 - 1}{x - 1}$. *Ans.* 1.

(b) $x^n - 1$ (n odd) and $x^2 + 1$. *Ans.* 2.

(c) $x^n + x + 1$ and $x^2 - 3x + 2$.

(d) $x^n + 1$ and $(x - 1)^n$.

(e) $x^n - a^n$ and $x^n - b^n$.

2. Find the discriminant of

(a) $ax^2 + bx + c$. *Ans.* $b^2 - 4ac$.

(b) $x^3 + 3Hx + G$. *Ans.* $-27(G^2 + 4H^3)$.

(c) $x^n + t$.

(d) $(x^n - 1)(x^m - 1)$.

3. Let $A(x)$ be a polynomial of degree $n \geq 2$ with real coefficients and no multiple roots. Prove that if $A(x)$ has r real roots and s pairs of conjugate imaginary roots ($r + 2s = n$), then $D(A)$ is positive or negative according as s is even or odd. [Use (4).]

4. Prove that $\rho(A, A + B) = \rho(A, B)$. [Use Theorem 5.]

47. Symmetric functions. A function of two or more variables is called a *symmetric function* of these variables if it is unaltered when the variables are permuted in all possible ways. For example, the functions

$$x_1^3 + x_2^3 + x_3^3,$$
$$(x_1 - x_2)^2(x_2 - x_3)^2(x_3 - x_1)^2$$

are symmetric functions of x_1, x_2, and x_3; but the function

$$x_1 + x_2^2 + x_3$$

is not a symmetric function since it is changed into a different function when x_1 and x_2 are interchanged.

The function $\cos(x - y)$ is a symmetric function of x and y but will not be considered in our work. We shall confine our attention to polynomials exclusively.

We have already encountered the symmetric functions

$$\begin{aligned} \sigma_1 &= \Sigma x_1 = x_1 + x_2 + \cdots + x_n, \\ \sigma_2 &= \Sigma x_1x_2 = x_1x_2 + x_1x_3 + \cdots + x_{n-1}x_n, \\ &\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ \sigma_n &= x_1x_2 \cdots x_n, \end{aligned}$$

of $x_1, x_2, \cdots, x_n$. They are called the *elementary symmetric functions* of these variables, and σ_k is called the kth elementary symmetric function.

The example

$$\begin{aligned} x_1^2 + x_2^2 + \cdots + x_n^2 &= (x_1 + x_2 + \cdots + x_n)^2 \\ &\qquad - 2(x_1x_2 + \cdots + x_{n-1}x_n) \\ &= \sigma_1^2 - 2\sigma_2 \end{aligned}$$

illustrates the fundamental theorem on symmetric functions: *Every symmetric function is expressible in terms of the elementary symmetric functions* (stated more precisely in § 49), which we proceed to prove.

48. Functional independence of the elementary symmetric functions. The polynomials

$$f_k(x_1, x_2, \cdots, x_n), \qquad (k = 1, 2, \cdots, r)$$

are *functionally dependent* relative to a field R if there exists a polynomial $F(z_1, \cdots, z_r)$ in R, different from 0, such that

$$F[f_1(x_1, \cdots, x_n), \cdots, f_r(x_1, \cdots, x_n)] = 0.$$

In the contrary case the functions are *functionally independent* relative to R.

Example. The functions

$$f_1 = x_1^2 + x_2^2, \quad f_2 = x_1^2 - x_2^2, \quad f_3 = x_1x_2$$

are functionally dependent relative to $R(1)$ since

$$f_1^2 - f_2^2 - 4f_3^2 = 0.$$

In this example the function $F(z_1, z_2, z_3)$ referred to in the definition is $z_1^2 - z_2^2 - 4z_3^2$.

THEOREM 7. *The elementary symmetric functions of n independent variables are functionally independent relative to any field which contains none of these variables.*

Let

$$(1)\quad F(z_1, \cdots, z_n) = \sum_{q_1, q_2, \cdots, q_n} c_{q_1q_2\cdots q_n} z_1^{q_1} z_2^{q_2} \cdots z_n^{q_n} \neq 0$$

be a polynomial in a field R containing none of the variables $x_1, \cdots, x_n$. It is assumed that the right member of (**1**) has the *reduced* form in which no two distinct terms have exactly the same exponents of $z_1, z_2, \cdots, z_n$. Let $\sigma_1, \cdots, \sigma_n$ be the elementary symmetric functions of $x_1, \cdots, x_n$. We are to prove that $F(\sigma_1, \cdots, \sigma_n) \neq 0$.

Of the terms of (**1**) consider those for which $q_1 + q_2 + \cdots + q_n$ is a maximum; and of these select those for which $q_2 + \cdots + q_n$ is a maximum; of these select those for which $q_3 + \cdots + q_n$ is a maximum; etc. There can be only one term which meets all these requirements; for if

$$\begin{aligned} q_1 + q_2 + \cdots + q_n &= q_1' + q_2' + \cdots + q_n', \\ q_2 + \cdots + q_n &= q_2' + \cdots + q_n', \\ &\cdots\cdots \\ q_{n-1} + q_n &= q'_{n-1} + q_n', \\ q_n &= q_n', \end{aligned}$$

then

$$q_n = q_n', \; q_{n-1} = q'_{n-1}, \; \cdots, \; q_1 = q_1'.$$

Let $c_{q_1q_2\cdots q_n} z_1^{q_1} z_2^{q_2} \cdots z_n^{q_n}$ be this unique term. We have

$$\sigma_1^{q_1}\sigma_2^{q_2} \cdots \sigma_n^{q_n} = (x_1 + \cdots + x_n)^{q_1} (x_1x_2 + \cdots + x_{n-1}x_n)^{q_2} \cdots (x_1 \cdots x_n)^{q_n}.$$

Therefore one of the terms which occurs when

$$c_{q_1 q_2 \cdots q_n} \sigma_1^{q_1} \sigma_2^{q_2} \cdots$$

is expressed in terms of $x_1, \cdots, x_n$ is

$$
\begin{aligned}
(2) \quad & c_{q_1 q_2 \cdots q_n} x_1^{q_1} (x_1 x_2)^{q_2} \cdots (x_1 x_2 \cdots x_n)^{q_n} \\
& = c_{q_1 q_2 \cdots q_n} x_1^{q_1 + q_2 + \cdots + q_n} x_2^{q_2 + \cdots + q_n} \cdots x_{n-1}^{q_{n-1} + q_n} x_n^{q_n};
\end{aligned}
$$

and no other term has the same exponents. Moreover, in view of the maximal conditions imposed on $q_1, \cdots, q_n$, no term whose exponents are the same as those of the right member of (2) can arise when any other term of $F(\sigma_1, \cdots, \sigma_n)$ is expressed in terms of $x_1, \cdots, x_n$. Therefore, when $F(\sigma_1, \cdots, \sigma_n)$ is expressed in terms of $x_1, \cdots, x_n$, and simplified by combining like terms, the right member of (2) will actually occur since it does not combine with any other term. We conclude that $F(\sigma_1, \cdots, \sigma_n) \neq 0$.

49. The fundamental theorem on symmetric functions.* A polynomial in n variables $x_1, \cdots, x_n$ in a field R consists of the sum of a finite number of monomials such as $cx_1^{p_1}x_2^{p_2} \cdots x_n^{p_n}$, where c is an element of R and the p's are non-negative integers. If this monomial is a term of a symmetric function, every monomial obtained from it by permuting the x's in all possible ways is also a term of the symmetric function. Therefore *every symmetric polynomial equals a linear combination of Σ-functions.* By a Σ-function we mean a symmetric function which is the sum of all the distinct monomials obtained from a given monomial by permuting the variables in all possible ways. A Σ-function is determined by any one of its terms. The Σ-function determined by $x_1^{p_1}x_2^{p_2} \cdots x_n^{p_n}$ is denoted by

$$(1) \qquad \Sigma x_1^{p_1} x_2^{p_2} \cdots x_n^{p_n}.$$

We proceed to prove that (1) is expressible in terms of the elementary symmetric functions of $x_1, \cdots, x_n$.

Let $x_1', x_2', \cdots, x_m'$ be m variables independent of one another and of $x_1, \cdots, x_n$, m being greater than the largest of the exponents in (1). Construct the polynomials

$$
\begin{aligned}
(2) \quad A(x) &= (x - x_1) \cdots (x - x_n) \\
&= x^n - \sigma_1 x^{n-1} + \sigma_2 x^{n-2} - \cdots + (-1)^n \sigma_n,
\end{aligned}
$$

* The proof which follows is due to M. Faber, *Archiv der Mathematik und Physik,* Vol. 16 (1910), p. 144.

$$(3)\quad B(x) = (x + x_1') \cdots (x + x_m') = x^m + \sigma_1' x^{m-1} + \sigma_2' x^{m-2} + \cdots + \sigma_m'.$$

By Theorem 5,

$$\begin{aligned}(4)\quad \rho(A, B) &= B(x_1)B(x_2) \cdots B(x_n)\\ &= (x_1^m + \sigma_1' x_1^{m-1} + \sigma_2' x_1^{m-2} + \qquad + \sigma_m')\\ &\times (x_2^m + \sigma_1' x_2^{m-1} + \sigma_2' x_2^{m-2} + \qquad + \sigma_m')\\ &\times (x_n^m + \sigma_1' x_n^{m-1} + \sigma_2' x_n^{m-2} + \cdots + \sigma_m').\end{aligned}$$

The coefficient of $\sigma'_{m-p_1}\sigma'_{m-p_2} \cdots \sigma'_{m-p_n}$ *in the expansion of the last member of* (**4**) *is precisely the* Σ*-function* (**1**). The reader may verify this statement by studying the law of combination of the terms of the expansion, noting that the coefficient of σ'_{m-p_k} in the lth line of the last member of (**4**) is $x_l^{p_k}$.

On the other hand, the coefficient of $\sigma'_{m-p_1}\sigma'_{m-p_2} \cdots \sigma'_{m-p_n}$ in the first member of (**4**) is a polynomial in $\sigma_1, \sigma_2, \cdots \sigma_n$ with integral coefficients; for $\rho(A, B)$ is a polynomial, with integral coefficients, in $\sigma_1, \sigma_2, \cdots, \sigma_n, \sigma_1', \sigma_2', \quad , \sigma_m'$. Since, by Theorem 7, $\sigma_1', \sigma_2', \cdots, \sigma_m'$ are functionally independent relative to $R(x_1, x_2, \cdots, x_n)$, we may equate coefficients. Therefore (**1**) equals a polynomial, with integral coefficients, in $\sigma_1, \sigma_2, \cdots, \sigma_n$.

THEOREM 8. *Every Σ-function of n independent variables can be expressed in one, and in only one, way as a polynomial, with integral coefficients, in the elementary symmetric functions of these variables.*

THEOREM 9. *Every rational integral symmetric function of n variables, with integral coefficients, can be expressed in one, and in only one, way as a polynomial, with integral coefficients, in the elementary symmetric functions of these variables.*

THEOREM 10. (FUNDAMENTAL THEOREM ON SYMMETRIC FUNCTIONS). *Every rational integral symmetric function of n variables, in a field R, can be expressed in one, and in only one, way as a polynomial, with coefficients in R, in the elementary symmetric functions of these variables.*

In each of these theorems the uniqueness of the indicated polynomial follows from Theorem 7.

50. Degree and weight of a symmetric function. When the variables $x_1, \cdots, x_n$ are permuted in any manner, the monomial $x_1^{p_1}x_2^{p_2} \cdots x_n^{p_n}$ is transformed into a monomial of the form

$x_{v_1}^{p_1}x_{v_2}^{p_2}\cdots x_{v_n}^{p_n}$, where $v_1, v_2, \cdots, v_n$ are the integers $1, 2, \cdots, n$ in some order or other. The sum of the exponents of each of these monomials is the same number $p_1 + p_2 + \cdots + p_n$. Therefore, *every non-homogeneous symmetric polynomial equals the sum of two or more homogeneous symmetric polynomials.*

The *degree* of a symmetric function is its degree in any *one* of the variables. The *weight* of a homogeneous symmetric function is its degree in *all* the variables. For example, the degree of the Σ-function $\Sigma x_1^{p_1}x_2^{p_2}\cdots x_n^{p_n}$ is the largest of the exponents $p_1, p_2, \cdots, p_n$; its weight is $p_1 + p_2 + \cdots + p_n$. Again, each of the elementary symmetric functions is of degree 1, while the kth elementary symmetric function is of weight k.

Let $f(x_1, \cdots, x_n)$ be a homogeneous symmetric function, and let its expression in terms of the elementary symmetric functions be

$$(1)\qquad f(x_1, \cdots, x_n) = \Sigma c_{q_1q_2\cdots q_n}\sigma_1^{q_1}\sigma_2^{q_2}\cdots\sigma_n^{q_n}.$$

We wish to compute the degree θ and the weight w of

$$f(x_1, \cdots, x_n)$$

by means of the right member of (1).

When each of the σ's in (1) is expressed in terms of the x's, (1) becomes an identity in the x's. Let us replace $x_1, \cdots, x_n$ by $tx_1, \cdots, tx_n$ respectively, t being a new variable. Then σ_k becomes $t^k\sigma_k$, and

$$(2)\quad f(tx_1, \cdots, tx_n) = \Sigma c_{q_1q_2\cdots q_n}t^{q_1+2q_2+\cdots+nq_n}\sigma_1^{q_1}\sigma_2^{q_2}\cdots\sigma_n^{q_n}.$$

But

$$(3)\qquad f(tx_1, \cdots, tx_n) = t^w f(x_1, \cdots, x_n).$$

Therefore

$$(4)\qquad w = q_1 + 2q_2 + \cdots + nq_n,$$

this number being necessarily the same for each term of the right member of (1). When this condition is not satisfied the right member of (1) does not represent a homogeneous symmetric function.

Of the terms of the right member of (1), select those for which $q_1 + q_2 + \cdots + q_n$ is a maximum; of these select those for

which $q_2 + \cdots + q_n$ is a maximum; etc. We saw in § 48 that only one term satisfies these requirements. Denoting this term by $c_{q_1q_2 \ldots q_n}\sigma_1^{q_1}\sigma_2^{q_2} \cdots \sigma_n^{q_n}$, we also saw that one of the terms which occurs in the expansion of this expression is

$$c_{q_1q_2 \ldots q_n}x_1^{q_1+q_2+\cdots+q_n}x_2^{q_2+\cdots+q_n} \cdots x_{n-1}^{q_{n-1}+q_n}x_n^{q_n}$$

and that no other term with the same exponents could occur in the expansion of the right member of (1). Therefore x_1 actually occurs to the $(q_1 + q_2 + \cdots + q_n)$th power in $f(x_1, \cdots, x_n)$ and evidently to no higher power. The degree of $f(x_1, \cdots, x_n)$ is therefore the maximum value of $q_1 + q_2 + \cdots + q_n$.

THEOREM 11. *If* $\Sigma c_{q_1q_2 \ldots q_n}\sigma_1^{q_1}\sigma_2^{q_2} \cdots \sigma_n^{q_n}$ *represents a homogeneous symmetric function of* $x_1, \cdots, x_n$, *of degree* θ *and weight* w, σ_k *denoting the kth elementary symmetric function of* $x_1, \cdots, x_n$, *then* θ *is the maximum value of* $q_1 + q_2 + \cdots + q_n$ *and* $w = q_1 + 2q_2 + \cdots + nq_n$.

51. Evaluation of symmetric functions. Simple symmetric functions can be evaluated (expressed in terms of the elementary symmetric functions) by algebraic manipulation. For example,

$$\Sigma x_1^2 = x_1^2 + \cdots x_n^2 = (x_1 + \cdots + x_n)^2 - 2\Sigma x_1x_2$$
$$= \sigma_1^2 - 2\sigma_2;$$
$$\Sigma x_1^3 = (\Sigma x_1)^3 - 3\Sigma x_1 \times \Sigma x_1x_2 + 3\Sigma x_1x_2x_3 = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3.$$

Algebraic manipulation is clearly unsatisfactory when the symmetric function is sufficiently complicated. The methods illustrated in the following examples will then be found serviceable.

Example 1. Evaluate the symmetric function

$$(x_1 - x_2)^2(x_2 - x_3)^2(x_3 - x_1)^2$$

of x_1, x_2, and x_3.

The weight and degree of this symmetric function are $w = 6$ and $\theta = 4$ respectively. The integer 6 is first *partitioned* in all possible ways into a sum of at most 4 smaller positive integers, none of which exceeds 3 (3 being the number of variables). The only possible partitions are

$$6 = 3 + 3 = 3 + 2 + 1 = 3 + 1 + 1 + 1$$
$$= 2 + 2 + 2 = 2 + 2 + 1 + 1.$$

Corresponding to these partitions we form the functions

$$\sigma_3^2, \quad \sigma_1\sigma_2\sigma_3, \quad \sigma_1^3\sigma_3, \quad \sigma_2^3, \quad \sigma_1^2\sigma_2^2$$

respectively, each of which is of weight 6 and degree ≤ 4. There are other partitions of the number 6 such as $2 + 1 + 1 + 1 + 1$ and $4 + 2$. The first of these is rejected because the corresponding symmetric function $\sigma_1^4\sigma_2$ is of degree 5; the second is rejected because the corresponding symmetric function is $\sigma_2\sigma_4$ and there is no σ_4 in the present example.

We now write

$$(1) \quad (x_1 - x_2)^2(x_2 - x_3)^2(x_3 - x_1)^2 = l_1\sigma_3^2 + l_2\sigma_1\sigma_2\sigma_3 + l_3\sigma_1^3\sigma_3 + l_4\sigma_2^3 + l_5\sigma_1^2\sigma_2^2.$$

The right member represents the *most general* homogeneous symmetric of 3 variables of weight 6 and degree 4. Our problem reduces to that of determining the l's (which are integers by Theorem 9) so that (**1**) is satisfied. We do so by a judicious choice of cubic equations whose roots are known.

(a) $x^3 - 1 = 0$; $x_1 = 1$, $x_2 = \omega$, $x_3 = \omega^2$; $\sigma_1 = 0$, $\sigma_2 = 0$, $\sigma_3 = 1$;

where ω and ω^2 are the imaginary cube roots of unity. Bearing in mind that $1 + \omega + \omega^2 = 0$ and that $\omega^3 = 1$, we find that

$$\begin{aligned}(x_1 - x_2)^2 &= (1 - \omega)^2 = 1 - 2\omega + \omega^2 = -3\omega,\\ (x_2 - x_3)^2 &= (\omega - \omega^2)^2 = \omega^2 - 2 + \omega = -3,\\ (x_3 - x_1)^2 &= (\omega^2 - 1)^2 = \omega - 2\omega^2 + 1 = -3\omega^2.\end{aligned}$$

Substituting in (**1**) we have

$$(2) \qquad -27 = l_1.$$

$$\text{(b)} \qquad x^3 - x = 0; x_1 = 0, x_2 = 1, x_3 = -1; \quad \sigma_1 = 0, \sigma_2 = -1, \sigma_3 = 0.$$

Substituting in (**1**) we have $(-1)^2 \cdot 2^2(-1)^2 = -l_4$. Therefore

$$(3) \qquad l_4 = -4.$$

$$\text{(c)} \qquad x^3 - 2x^2 + x = 0; x_1 = 0, x_2 = 1, x_3 = 1; \quad \sigma_1 = 2, \sigma_2 = 1, \sigma_3 = 0.$$

Substituting in (**1**) we have $0 = l_4 + 4l_5$. Therefore, by (**3**),

$$(4) \qquad l_5 = 1.$$

$$\text{(d)} \qquad x^3 - 2x^2 - x + 2 = 0; x_1 = 1, x_2 = -1, x_3 = 2; \quad \sigma_1 = 2, \sigma_2 = -1, \sigma_3 = -2.$$

Hence

$$36 = 4l_1 + 4l_2 - 16l_3 - l_4 + 4l_5.$$

It follows from the preceding results that

(5) $$l_2 - 4l_3 = 34.$$

(e) $$x^3 - 3x^2 + 3x - 1 \quad 0; x_1 = x_2 = x_3 = 1;$$
$$\sigma_1 = 3,\ \sigma_2 = 3,\ \sigma_3 = 1.$$

Hence

$$0 = l_1 + 9l_2 + 27l_3 + 27l_4 + 81l_5,$$

so that

(6) $$l_2 + 3l_3 = 6.$$

Solving (5) and (6) we obtain $l_2 = 18$ and $l_3 = -4$. Therefore

$$(x_1 - x_2)^2(x_2 - x_3)^2(x_3 - x_1)^2 = -27\sigma_3^2 + 18\sigma_1\sigma_2\sigma_3 - 4\sigma_1^3\sigma_3 - 4\sigma_2^3 + \sigma_1^2\sigma_2^2.$$

Example 2. Evaluate $\Sigma x_1^2x_2^2x_3^2x_4x_5$, the number of variables n being arbitrary.

Here $w = 8$ and $\theta = 2$, and

$$8 = 8 = 7 + 1 = 6 + 2 = 5 + 3 = 4 + 4.$$

Therefore

(7) $$\Sigma x_1^2x_2^2x_3^2x_4x_5 = l_1\sigma_8 + l_2\sigma_1\sigma_7 + l_3\sigma_2\sigma_6 + l_4\sigma_3\sigma_5 + l_5\sigma_4^2,$$

where the l's are integers to be determined. Since $x_1, \quad , x_n$ satisfy the equation

(8) $$x^n - \sigma_1x^{n-1} + \quad + (-1)^n\sigma_n = 0,$$

and $\sigma_9, \sigma_{10}, \cdots$ do not appear in the right member of (7), we take $\sigma_9 = 0$, $\sigma_{10} = 0, \cdots$, without affecting (7). Then (8) becomes

(9) $$x^n - \sigma_1x^{n-1} + \cdots + \sigma_8x^{n-8} = 0,$$

which has $n - 8$ roots equal to 0. Therefore, *the right member of* (7) *is the same for every* $n \geq 8$. In other words, the l's are independent of n. We shall therefore assume that there are only 8 x's in the left member of (7).

We first choose $x_5 = x_6 = x_7 = x_8 = 0$; hence $\sigma_5 = \sigma_6 = \sigma_7 = \sigma_8 = 0$. Substituting in (7) we have $0 = l_5\sigma_4^2$, so that $l_5 = 0$.

Next, choose $x_6 = x_7 = x_8 = 0$; hence $\sigma_6 = \sigma_7 = \sigma_8 = 0$. Each term of the left member of (7) is divisible by $x_1x_2x_3x_4x_5 = \sigma_5$. Cancelling, we obtain $\Sigma x_1x_2x_3 = l_4\sigma_3$. Therefore $l_4 = 1$.

Now take $x_7 = x_8 = 0$ and the other x's $= 1$. As these x's satisfy the equation

$$x^2(x-1)^6 = x^8 - 6x^7 + 15x^6 - 20x^5 + 15x^4 - 6x^3 + x^2 = 0,$$
$$\sigma_1 = 6, \sigma_2 = 15, \sigma_3 = 20, \sigma_4 = 15, \sigma_5 = 6, \sigma_6 = 1, \sigma_7 = 0, \sigma_8 = 0.$$

Each term of the left member of (7) has the form $(x_ax_bx_c)^2x_dx_e$, whose subscripts are five of the first six natural numbers, if we neglect terms which vanish. There are $(6 \cdot 5 \cdot 4)/(1 \cdot 2 \cdot 3) = 20$ choices for the triad $x_ax_bx_c$. After one of these has been selected there are $(3 \cdot 2)/(1 \cdot 2) = 3$ choices for the pair x_dx_e. The left member of (7) therefore consists of $20 \times 3 = 60$ non-vanishing terms, each of which has the value 1. Hence $60 = 15l_3 + 120$, since $l_4 = 1$; therefore $l_3 = -4$.

Next, take $x_8 = 0$ and the other x's $= 1$. As the first seven x's satisfy the equation

$$(x-1)^7 = x^7 - 7x^6 + 21x^5 - 35x^4 + 35x^3 - 21x^2 + 7x - 1 = 0,$$
$$\sigma_1 = 7, \sigma_2 = 21, \sigma_3 = 35, \sigma_4 = 35, \sigma_5 = 21, \sigma_6 = 7, \sigma_7 = 1, \sigma_8 = 0.$$

The number of non-vanishing terms in the left member of (7) is now $(7 \cdot 6 \cdot 5)/(1 \cdot 2 \cdot 3) \times (4 \cdot 3)/(1 \cdot 2) = 210$, and each of these terms has the value 1. Therefore

$$210 = 7l_2 - 4 \cdot 21 \cdot 7 + 35 \cdot 21,$$

and $l_2 = 9$.

Finally, take all the x's $= 1$, satisfying the equation

$$(x-1)^8 = x^8 - 8x^7 + 28x^6 - 56x^5 + 70x^4 - 56x^3 + 28x^2 - 8x + 1 = 0.$$

Here $\sigma_1 = 8, \sigma_2 = 28, \sigma_3 = 56, \sigma_4 = 70, \sigma_5 = 56, \sigma_6 = 28, \sigma_7 = 8, \sigma_8 = 1$.

The number of terms in the left member of (7) is $(8 \cdot 7 \cdot 6)/(1 \cdot 2 \cdot 3) \times (5 \cdot 4)/(1 \cdot 2) = 560$. Therefore

$$560 = l_1 + 9 \cdot 64 - 4 \cdot 28 \cdot 28 + 56 \cdot 56,$$

and $l_1 = -16$. We conclude that

$$\Sigma x_1^2x_2^2x_3^2x_4x_5 = -16\sigma_8 + 9\sigma_1\sigma_7 - 4\sigma_2\sigma_6 + \sigma_3\sigma_5.$$

EXERCISES

Show that the following symmetric functions have the indicated evaluations.

1. $(x_1^2 + x_2^2)(x_2^2 + x_3^2)(x_3^2 + x_1^2)$
$$= -\sigma_3^2 + 4\sigma_1\sigma_2\sigma_3 - 2\sigma_2^3 - 2\sigma_1^3\sigma_3 + \sigma_1^2\sigma_2^2.$$
2. $(x_1^2x_2 + x_2^2x_3 + x_3^2x_1)(x_1x_2^2 + x_2x_3^2 + x_3x_1^2)$
$$= 9\sigma_3^2 + \sigma_1^3\sigma_3 + \sigma_2^3 - 6\sigma_1\sigma_2\sigma_3.$$
3. $(x_1 + x_2 - x_3 - x_4)(x_1 - x_2 + x_3 - x_4)(x_1 - x_2 - x_3 + x_4)$
$$= 8\sigma_3 - 4\sigma_1\sigma_2 + \sigma_1^3.$$
4. $(x_1x_2 + x_3x_4)(x_1x_3 + x_2x_4)(x_1x_4 + x_2x_3) = -4\sigma_2\sigma_4 + \sigma_1^2\sigma_4 + \sigma_3^2.$
5. $\Sigma x_1^2x_2 = -3\sigma_3 + \sigma_1\sigma_2.$
6. $\Sigma x_1^2x_2^2 = 2\sigma_4 - 2\sigma_1\sigma_3 + \sigma_2^2.$
7. $\Sigma x_1^2x_2x_3 = -4\sigma_4 + \sigma_1\sigma_3.$
8. $\Sigma x_1^2x_2^2x_3 = 5\sigma_5 - 3\sigma_1\sigma_4 + \sigma_2\sigma_3.$
9. $\Sigma x_1^2x_2^2x_3x_4 = 9\sigma_6 - 4\sigma_1\sigma_5 + \sigma_2\sigma_4.$
10. $\Sigma x_1^4 = -4\sigma_4 + 4\sigma_1\sigma_3 + 2\sigma_2^2 - 4\sigma_1^2\sigma_2 + \sigma_1^4.$

52. The symmetric function s_k. Newton's identities. The sum of the kth powers of n variables is a symmetric function of these variables of particular interest and may be evaluated with the aid of the following theorem.

THEOREM 12. *Let $f(x) = a_0(x - x_1)(x - x_2) \cdots (x - x_n)$ $(a_0 \neq 0)$, and let $s_k = x_1^k + x_2^k + \cdots + x_n^k$. The quotient of the division of the polynomial $x^{k+1}f'(x)$ by $f(x)$ is*

$$s_0x^k + s_1x^{k-1} + s_2x^{k-2} + \cdots + s_{k-1}x + s_k, \qquad (s_0 = n).$$

We are to prove that

$$(1) \quad x^{k+1}f'(x) = (s_0x^k + s_1x^{k-1} + \cdots + s_{k-1}x + s_k)f(x) + g(x),$$

where $g(x)$ is either 0 or a polynomial of degree $\leq n - 1$. Differentiating

$$f(x) = a_0(x - x_1)(x - x_2) \cdots (x - x_n),$$

and multiplying by x^{k+1}, we have

$$x^{k+1}f'(x) = \frac{x^{k+1}f(x)}{x - x_1} + \frac{x^{k+1}f(x)}{x - x_2} + \cdots + \frac{x^{k+1}f(x)}{x - x_n}$$
$$= \sum_{i=1}^{n} \frac{x^{k+1}f(x)}{x - x_i} = \sum_{i=1}^{n} \frac{(x^{k+1} - x_i^{k+1} + x_i^{k+1})f(x)}{x - x_i}$$
$$= f(x)\sum_{i=1}^{n} \frac{x^{k+1} - x_i^{k+1}}{x - x_i} + \sum_{i=1}^{n} \frac{x_i^{k+1}f(x)}{x - x_i}.$$

The degree of the polynomial

$$g(x) = \sum_{i=1}^{n} \frac{x_i^{k+1} f(x)}{x - x_i}$$

is clearly $\leq n - 1$. The quotient of the division of $x^{k+1}f'(x)$ by $f(x)$ is therefore

$$\begin{aligned} \sum_{i=1}^{n} \frac{x^{k+1} - x_i^{k+1}}{x - x_i} &= \sum_{i=1} (x^k + x_i x^{k-1} + \quad + x_i^{k-1}x + x_i^k) \\ &= nx^k + (\Sigma x_1)x^{k-1} + \cdots + (\Sigma x_1^{k-1})x + \Sigma x_1^k \\ &= s_0 x^k + s_1 x^{k-1} + \cdots + s_{k-1}x + s_k. \end{aligned}$$

We now suppose that $f(x)$ is a primary polynomial, so that

$$f(x) = x^n + c_1 x^{n-1} + \cdots + c_{n-1}x + c_n,$$

where

$$c_1 = -\sigma_1, c_2 = \sigma_2, \cdots, c_n = (-1)^n \sigma_n.$$

Written at length (**1**) becomes

$$\begin{aligned} & nx^{n+k} + (n-1)c_1 x^{n+k-1} + \quad \cdot + 2c_{n-2}x^{k+2} + c_{n-1}x^{k+1} \\ (2) \qquad & = (s_0 x^k + s_1 x^{k-1} + \quad \cdot + s_{k-1}x + s_k) \\ & \times (x^n + c_1 x^{n-1} + \cdot \quad + c_{n-1}x + c_n) + g(x). \end{aligned}$$

Equating coefficients of x^n, observing that the coefficient of x^n in the left member of (**2**) is $(n - k)c_k$ if $k \leq n$ and is 0 if $k > n$, we have

$$s_k + c_1 s_{k-1} + c_2 s_{k-2} + \cdot \quad + c_{k-1}s_1 + nc_k = (n - k)c_k, \; (k \leq n),$$

$$(3) \quad \mathbf{s_k + c_1 s_{k-1} + c_2 s_{k-2} + \quad \cdot + c_{n-1} s_{k-n+1} + c_n s_{k-n} = 0, \quad (k > n).}$$

The first of these equations may be simplified, yielding *Newton's identities:*

$$(4) \quad \mathbf{s_k + c_1 s_{k-1} + c_2 s_{k-2} + \cdots + c_{k-1} s_1 + kc_k = 0, \quad (k = 1, \cdots, n).}$$

The symmetric functions $s_1, s_2, \cdots$ may be successively computed by means of (**4**) and (**3**) in terms of $c_1, c_2, \cdots, c_n$ or $\sigma_1, \sigma_2, \cdots, \sigma_n$. They may also be computed by means of Theorem 12.

EXERCISES

1. With the notation of the text, show that the leading coefficient of $g(x)$ is a_0s_{k+1}.

2. Show that

$$g(x_i) = x_i^{k+1}f'(x_i), \qquad (i = 1, \cdots, n).$$

3. Deduce (3) from

$$x_1^{k-n}f(x_1) + x_2^{k-n}f(x_2) + \cdots + x_n^{k-n}f(x_n) = 0.$$

4. Verify the indicated value of s_k for the roots of each of the following polynomials:

(a) $x^4 + 5x^3 + 2x^2 - 8x - 7,\quad s_3 = -71.$

(b) $x^3 - x^2 - 2x + 1,\quad s_4 = -3.$

(c) $x^n - nx + t\ (n \geq 5),\quad s_3 = 0,\ s_n = -nt.$

5. To find the value of s_{-k} for the roots of $f(x)$, find the value of s_k for the roots of the polynomial whose roots are the reciprocals of the roots of $f(x)$. Verify the following:

(a) $x^4 + x + 1,\quad s_{-3} = -1.$

(b) $x^2 - ix + 2,\quad s_{-3} = -7i/8.$

6. Show that

(a) $s_2 = \sigma_1^2 - 2\sigma_2.$

(b) $s_3 = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3.$

(c) $s_4 = \sigma_1^4 - 4\sigma_1^2\sigma_2 + 4\sigma_1\sigma_3 + 2\sigma_2^2 - 4\sigma_4.$

7. Show that

(a) $\sigma_2 = \frac{1}{2}(s_1^2 - s_2).$

(b) $\sigma_3 = \frac{1}{6}(s_1^3 - 3s_1s_2 + 2s_3).$

(c) $\sigma_4 = \frac{1}{24}(s_1^4 - 6s_1^2s_2 + 8s_1s_3 + 3s_2^2 - 6s_4).$

53. Miscellaneous problems. The theory of symmetric functions may be employed to great advantage in the solution of problems such as the following:

Example 1. Find the condition that two roots of the equation

$$a_0x^3 + a_1x^2 + a_2x + a_3 = 0$$

be equal.

Denote the roots by x_1, x_2, x_3. In order that two roots be equal it is necessary and sufficient that $(x_1 - x_2)(x_2 - x_3)(x_3 - x_1) = 0$. But the left member of this equation is not a symmetric function. The square of this function is, however, a symmetric function, and its vanishing is also a necessary and sufficient condition that the cubic have a pair of equal roots. We have seen (§ 51) that

$$(x_1 - x_2)^2(x_2 - x_3)^2(x_3 - x_1)^2 = -27\sigma_3^2 + 18\sigma_1\sigma_2\sigma_3 - 4\sigma_1^3\sigma_3 - 4\sigma_2^3 + \sigma_1^2\sigma_2^2$$

$$\frac{-27a_0^2a_3^2 + 18a_0a_1a_2a_3 - 4a_1^3a_3 - 4a_0a_2^3 + a_1^2a_2^2}{a_0^4}$$

whose numerator, it will be observed, is a *homogeneous* function of the a's. The required condition is

$$\mathbf{-27a_0^2a_3^2 + 18a_0a_1a_2a_3 - 4a_1^3a_3 - 4a_0a_2^3 + a_1^2a_2^2 = 0.}$$

Example 2. Find the condition that the roots of a cubic equation form a geometric progression.

With the notation of Example 1, a necessary and sufficient condition is that $(x_1^2 - x_2x_3)(x_2^2 - x_1x_3)(x_3^2 - x_1x_2) = 0$, whose left member is a symmetric function of degree 4 and weight 6. Instead of expressing it first in terms of the σ's and then in terms of the a's, let us express it directly in terms of the a's, bearing in mind that a_i is of degree 1 and weight i. We have

$$\begin{aligned} a_0^4(x_1^2 - x_2x_3)&(x_2^2 - x_1x_3)(x_3^2 - x_1x_2) \\ &= l_1a_0^2a_3^2 + l_2a_0a_1a_2a_3 + l_3a_1^3a_3 + l_4a_0a_2^3 + l_5a_1^2a_2^2, \end{aligned}$$

in which a power of a_0 has been introduced, where necessary, to make each term of degree 4 in the a's.

We find that $l_1 = 0$, $l_2 = 0$, $l_3 = 1$, $l_4 = -1$, $l_5 = 0$. The required condition is therefore

$$\mathbf{a_1^3a_3 - a_0a_2^3 = 0.}$$

Example 3. Find the resultant of $A(x) = a_0x^2 + a_1x + a_2$ and $B(x) = b_0x^3 + b_1x^2 + b_2x + b_3$.

Let $A(x) = a_0(x - x_1)(x - x_2)$. By Theorem 5,

$$\begin{aligned} \rho(A, B) &= a_0^3B(x_1)B(x_2) \\ &= a_0^3(b_0x_1^3 + b_1x_1^2 + b_2x_1 + b_3)(b_0x_2^3 + b_1x_2^2 + b_2x_2 + b_3) \\ &= a_0^3b_0^2x_1^3x_2^3 + a_0^3b_0b_1(x_1^3x_2^2 + x_1^2x_2^3) \\ &+ a_0^3b_0b_2(x_1^3x_2 + x_1x_2^3) + a_0^3b_0b_3(x_1^3 + x_2^3) + a_0^3b_1^2x_1^2x_2^2 \\ &+ a_0^3b_1b_2(x_1^2x_2 + x_1x_2^2) + a_0^3b_1b_3(x_1^2 + x_2^2) + a_0^3b_2^2x_1x_2 \\ &+ a_0^3b_2b_3(x_1 + x_2) + a_0^3b_3^3. \end{aligned}$$

Now

$$x_1 + x_2 = -a_1/a_0,\ x_1x_2 = a_2/a_0;$$

$$x_1^3x_2^2 + x_1^2x_2^3 = x_1^2x_2^2(x_1 + x_2) = -a_1a_2^2/a_0^3;$$

$$x_1^3 + x_2^3 = (x_1 + x_2)^3 - 3x_1x_2(x_1 + x_2) = -\frac{a_1^3 - 3a_0a_1a_2}{a_0^3};$$

etc.

Therefore

$$\begin{aligned}\rho(A, B) = {} & a_0^3b_3^2 - a_0^2a_1b_2b_3 - 2a_0^2a_2b_1b_3 + a_0^2a_2b_2^2 + a_0a_1^2b_1b_3 \\ & + 3a_0a_1a_2b_0b_3 - a_0a_1a_2b_1b_2 - 2a_0a_2^2b_0b_2 + a_0a_2^2b_1^2 \\ & - a_1a_2^2b_0b_1 + a_1^2a_2b_0b_2 - a_1^3b_0b_3 + a_2^3b_0^2.\end{aligned}$$

EXERCISES

1. Find the condition that the roots of a cubic equation form an arithmetic progression. *Ans.* $2a_1^3 - 9a_0a_1a_2 + 27a_0^2a_3 = 0$.
[The condition is $0 = (2x_1 - x_2 - x_3)(2x_2 - x_1 - x_3)(2x_3 - x_1 - x_2)$
$= (3x_1 + a_1/a_0)(3x_2 + a_1/a_0)(3x_3 + a_1/a_0)$
since $x_1 + x_2 + x_3 = -a_1/a_0$. Dividing each factor by -3, the condition becomes $f(-a_1/3a_0) = 0$ since $f(x) = a_0(x - x_1)(x - x_2)(x - x_3)$.]

2. Find the condition that the roots of a cubic equation form a harmonic progression.

3. Find the condition that one root of a quadratic equation be k times the other. *Ans.* $(k + 1)^2a_0a_2 - ka_1^2 = 0$.

4. Find the condition that one root of a quartic equation be equal to the sum of the other three. *Ans.* $16a_0^3a_4 - 8a_0^2a_1a_3 + 4a_0a_1^2a_2 - a_1^4 = 0$.
[Follow the method suggested in Ex. 1.]

5. Find the condition that the sum of two roots of a quartic equation be 0. *Ans.* $a_1^2a_4 + a_0a_3^2 - a_1a_2a_3 = 0$.

6. Find the resultant of $a_0x^2 + a_1x + a_2$ and $b_0x^2 + b_1x + b_2$.

7. Prove that $x^n + x^{-n} = f(x + x^{-1})$, where $f(y)$ is a polynomial with integral coefficients; and find $f(y)$ when $n = 2, 3, 4$.
Ans. $n = 2$, $f(y) = y^2 - 2$; $n = 3$, $f(y) = y^3 - 3y$;
$n = 4$, $f(y) = y^4 - 4y^2 + 2$.

8. Find the quadratic equation whose roots are

$$y_1 = x_1^2x_2 + x_2^2x_3 + x_3^2x_1, \quad y_2 = x_1x_2^2 + x_2x_3^2 + x_3x_1^2,$$

the x's being the roots of the equation $a_0x^3 + a_1x^2 + a_2x + a_3 = 0$.
Ans. $a_0^4y^2 + (a_0^2a_1a_2 - 3a_0^3a_3)y + 9a_0^2a_3^2 + a_0a_2^3 + a_1^3a_3 - 6a_0a_1a_2a_3 = 0$.

CHAPTER VII

ALGEBRAIC EXTENSIONS OF A FIELD

54. Methods of extending a field. A field is said to have been *extended* if a larger field has been found which contains the given field. The following examples show how fields may be extended:

1. If suitable definitions can be set up of the *convergence* and *limit* of a sequence of elements of a field R which is not compact (§ 30), the field may be extended by adding to R the limits of all convergent sequences of elements of R. The field of rational numbers may be extended in this way to the field of real numbers since every real number is the limit of at least one sequence of rational numbers; * and the field $R(i)$ to the field of complex numbers.

2. Let x be a variable not contained in a field R. The field $R(x)$ consisting of all rational functions of x with coefficients in R is a *transcendental* extension of R. Every field may be extended in this way.

3. Let α be a root of an irreducible equation of degree ≥ 2 in a field R. The field $R(\alpha)$ consisting of all rational functions of α with coefficients in R is an *algebraic* extension of R, obtained by *adjoining* α to R. The fields $R(x)$ and $R(\alpha)$ have essentially different properties because the powers of x satisfy no linear equation with coefficients in R, whereas certain powers of α do satisfy an equation of this type.

The algebraic extensions of a field are most important in the Theory of Equations and will be treated in this chapter.

55. Algebraic elements relative to a field. A root of a polynomial in a field R is called an *algebraic element* relative to R. If R is the field of rational numbers the root is called an *algebraic number*.† If R is the field of rational functions of one or more variables with coefficients in a number-field, the root is called an *algebraic function* of these variables.

* Consider, for example, the representation of a real number in the decimal system.

† But not every complex number is an algebraic number. See § 65.

Examples: 0, -1, $2\sqrt{7} + 4i$, and $\sqrt[3]{2}$ are algebraic numbers. $\sqrt[3]{x}$, $\sqrt{x_1 + x_2^{-3}}$, and $\sqrt{x_1 + i} - 3\sqrt{x_2 - \sqrt{2x_3}}$ are algebraic functions. There are, however, algebraic numbers and algebraic functions which are not expressible in terms of radicals.

An algebraic element relative to a field may or may not be an element of this field. The question of the *existence* of a root of a polynomial therefore arises. We shall see in the next chapter that if R is a number-field every polynomial in R of degree n has exactly n roots in the field of complex numbers. Therefore (§ 17) a polynomial of degree n in the field of complex numbers may be expressed in the form

$$(1) \qquad a_0(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n),$$

where a_0 is the leading coefficient of the polynomial and $\alpha_1, \alpha_2, \cdots, \alpha_n$ its roots (complex numbers). It is proved in works on the Theory of Functions that a polynomial of degree n in the field of rational functions of one or more variables, with coefficients in the field of complex numbers, has n roots, and may be expressed in the form (1) where $\alpha_1, \alpha_2, \cdots, \alpha_n$ are the roots (algebraic functions) of the polynomial. While these are the only cases we shall require, it may be pointed out that if R is any field, a field R' may be constructed such that every polynomial in R of degree n has n roots in R' and may be factored in R' as indicated by (1).

56. Conjugate elements and conjugate fields. Every algebraic element relative to a field R is clearly a root of more than one equation in R. Of all equations in R of which α, an algebraic element relative to R, is a root, *those of lowest degree are associates in* R. For if α is a root of each of the polynomials in R

$$A(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n, \qquad (a_0 \neq 0),$$

$$B(x) = b_0x^n + b_1x^{n-1} + \cdots + b_{n-1}x + b_n, \qquad (b_0 \neq 0),$$

and of no polynomial in R of degree $< n$, then α is a root of the polynomial

$$b_0A(x) - a_0B(x) = (b_0a_1 - a_0b_1)x^{n-1} + \cdots \\ + (b_0a_{n-1} - a_0b_{n-1})x + b_0a_n - a_0b_n,$$

which must be the zero-polynomial. It follows that $A(x)$ and $B(x)$ are associates in R.

If α is a root of an equation of degree n in R, but of no equation

in R of lower degree, α is of degree n relative to R; and the field $R(\alpha)$, consisting of all rational functions of α with coefficients in R, is an *algebraic field* of degree n relative to R. If $n = 1$, $R(\alpha) = R$. When $n = 2, 3, 4, \cdots$, $R(\alpha)$ is called a quadratic, cubic, quartic, $\cdots$ field respectively relative to R.

THEOREM 1. *If α is of degree n relative to R, an equation of degree n in R of which α is a root is irreducible in R.*

Let α be a root of the equation $A(x) = 0$ in R of degree n, and of no equation in R of lower degree. If $A(x)$ is reducible in R,

$$A(x) = B(x)C(x),$$

where $B(x)$ and $C(x)$ are polynomials in R of degree ≥ 1 and $\leq n - 1$. Since $A(\alpha) = B(\alpha)C(\alpha) = 0$, either $B(\alpha) = 0$ or $C(\alpha) = 0$; that is, α is a root of an equation in R of degree $< n$, contrary to hypothesis. Therefore $A(x)$ is irreducible in R.

THEOREM 2. *If a polynomial $f(x)$ in R has a root in common with a polynomial $A(x)$ which is irreducible in R, $f(x)$ is divisible by $A(x)$.* (The root in question need not be an element of R.)

If $A(x)$ and $f(x)$ are relatively prime, there exist two polynomials $U(x)$ and $V(x)$ in R such that

$$A(x)V(x) + f(x)U(x) = 1.$$

Let α be the common root of $A(x)$ and $f(x)$. Substituting $x = \alpha$, we obtain $0 = 1$. Therefore $A(x)$ and $f(x)$ are not relatively prime. Their g.c.d. must be $A(x)$ itself since $A(x)$ is irreducible in R and has no divisors in R besides constants and associates of $A(x)$. Therefore $f(x)$ is divisible by $A(x)$.

The primary irreducible polynomial in R of which a given algebraic element relative to R is a root is therefore unique, and is a divisor of every polynomial in R of which this element is a root.

We have seen (§ 20) that an irreducible equation has no multiple roots. Therefore if α is of degree n relative to R, the primary irreducible polynomial in R of which α is a root has exactly n roots

$$\alpha_1 = \alpha,\ \alpha_2,\ \cdots,\ \alpha_n,$$

all of which are distinct. Each of these roots is called a *conjugate* of any one of them relative to R. Each of the fields $R(\alpha_1)$, $R(\alpha_2)$, $\cdots$, $R(\alpha_n)$ is called a *conjugate* of any one of them relative to R.

Although conjugate elements are distinct, conjugate fields need not be distinct. For example, $\sqrt{2}$ and $-\sqrt{2}$ are conjugates relative

to $R(1)$, but $R(\sqrt{2}) = R(-\sqrt{2})$. Again, $\sqrt[4]{2}$, $-\sqrt[4]{2}$, $i\sqrt[4]{2}$ and $-i\sqrt[4]{2}$ are conjugates relative to $R(1)$, being the roots of the equation $x^4 = 2$, which is irreducible in $R(1)$; but $R(\sqrt[4]{2}) = R(-\sqrt[4]{2})$ and $R(i\sqrt[4]{2}) = R(-i\sqrt[4]{2})$, so that only two of the four conjugate fields are distinct.

THEOREM 3. *Every equation in R which is satisfied by an algebraic element relative to R is satisfied by every conjugate relative to R of that element.*

Let α be an algebraic element relative to R satisfying the irreducible equation $A(x) = 0$ in R, whose roots are $\alpha_1 = \alpha, \alpha_2, \cdots, \alpha_n$, the conjugates of α relative to R. If α is also a root of the equation $f(x) = 0$ in R, then, by Theorem 2,

$$f(x) = A(x)g(x),$$

$g(x)$ being a polynomial in R. Substituting $x = \alpha_i$, we obtain

$$f(\alpha_i) = A(\alpha_i)g(\alpha_i) = 0, \qquad (i = 1, \cdots, n).$$

EXERCISES

1. Find the degree of each of the following algebraic numbers by determining an irreducible equation in $R(1)$ satisfied by the number. Eisenstein's Irreducibility Theorem (§ 27) will be found useful.

(a) $\sqrt{-3 + \sqrt{7}}$.

(b) $\sqrt{3}(1 + i)$.

(c) $\sqrt[4]{2}(1 + i)/2$.

(d) $\sqrt{6 + 4\sqrt{2}} + \sqrt{6 - 4\sqrt{2}}$ (positive square roots).
Ans. 1; in fact, the given number is equal to 4.

(e) $\sqrt[n]{2}$.

(f) $\sqrt[3]{2 + \sqrt{5}} + \sqrt[3]{2 - \sqrt{5}}$. [Cube the number, observing that if $x = a + b$, then $x^3 = a^3 + b^3 + 3abx$.]

(g) $1 + \sqrt[3]{3} + \sqrt[3]{9}$. *Ans.* 3.

(h) $2\sqrt{2} + 3\sqrt{5}$.

2. Find the degree of $\sqrt{2} + \sqrt{3} + \sqrt{6}$ relative to $R(1)$; relative to $R(\sqrt{2})$; relative to $R(\sqrt{3})$; relative to $R(\sqrt{6})$.

3. Find the degree of $-i + \sqrt[3]{4}$ relative to $R(i)$; relative to $R(\sqrt[3]{2})$.

4. Find the degree of $\sqrt[3]{t} + \sqrt[3]{t^2}$ relative to $R(t)$, where t is a variable.

5. Prove that if an imaginary number is a root of an algebraic equation with real coefficients, its conjugate imaginary is also a root.

6. Show that an equation in the field of real numbers has an even number of imaginary roots.

7. Prove that if $a + b\sqrt{r}$ is an irrational root of an algebraic equation with rational coefficients, a and b being rational numbers, $a - b\sqrt{r}$ is also a root.

8. Does an algebraic equation with rational coefficients necessarily have an even number of irrational roots?

9. If $a + b\sqrt[3]{2}$ is a root of an algebraic equation with rational coefficients, does it follow that $a - b\sqrt[3]{2}$ is also a root?

10. Same question regarding $a + b\sqrt[4]{2}$.

11. Solve $x^4 + x^3 - 4x^2 - 5x - 5 = 0$, given that $\sqrt{5}$ is a root.

12. Solve $x^3 - 5x + 14\sqrt{3} = 0$, given that $\sqrt{3} + 2i$ is a root. Is $-\sqrt{3} + 2i$ a root?

13. Solve $x^3 - ix^2 + (-7 - i)x + 6 + 6i = 0$, given that $1 + i$ is a root. Is $1 - i$ a root?

14. Solve $x^4 - 3x^3 + 8x^2 + 17x - 13 = 0$, given that $2 - 3i$ is a root.

15. Solve $2x^5 - 3x^4 + 13x^3 - 14x^2 + 2 = 0$, given that $\sqrt[3]{2} - \sqrt[3]{4}$ is a root.

16. (a) What is the degree, relative to $R(1)$, of a primitive pth root of unity, p being a prime number?

(b) Prove that if the sum of k imaginary pth roots of unity (p prime) equals a rational number, then k is divisible by $p - 1$.

17. Let $A(x)$ be a polynomial of degree $n \geq 2$ which is irreducible in a field R. Prove that if the reciprocal of one root of $A(x)$ is a root of $A(x)$, then the reciprocal of *every* root of $A(x)$ is also a root. [Consider the polynomial $x^nA(x^{-1})$, and apply Theorem 2.]

18. With the same assumptions concerning $A(x)$, prove that if the negative of one root of $A(x)$ is a root of $A(x)$, then the negative of *every* root of $A(x)$ is also a root. Show further that $A(x)$ involves no odd powers of x.

19. Prove that if the polynomial $A(x)$ is irreducible in R, one root of $A(x)$ cannot be twice another. Generalize.

57. Canonical form of the elements of $R(\alpha)$. Primitive and imprimitive elements.

THEOREM 4. *If α is of degree n relative to R, every element of $R(\alpha)$ is expressible uniquely in the canonical form*

$$c_0\alpha^{n-1} + c_1\alpha^{n-2} + \ldots + c_{n-2}\alpha + c_{n-1},$$

*the c's being elements of R.**

Every element of $R(\alpha)$ is expressible in the form $f(\alpha)/g(\alpha)$ in at least one way, where $f(x)$ and $g(x)$ are polynomials in R and $g(x)$ is not divisible by $A(x)$, a polynomial in R or degree n having α as

* See § 8 for illustrations.

a root. Since $A(x)$ and $g(x)$ are relatively prime, there exist two polynomials $U(x)$ and $V(x)$ in R such that

$$A(x)U(x) + g(x)V(x) = 1.$$

Therefore

$$V(\alpha) = 1/g(\alpha),$$

and

$$f(\alpha)/g(\alpha) = f(\alpha)V(\alpha).$$

Let $Q(x)$ be the quotient and

$$C(x) = c_0x^{n-1} + c_1x^{n-2} + \cdots + c_{n-2}x + c_{n-1}$$

the remainder of the division of $f(x)V(x)$ by $A(x)$. We have

$$f(x)V(x) = Q(x)A(x) + C(x).$$

Consequently

$$\begin{aligned} f(\alpha)/g(\alpha) &= f(\alpha)V(\alpha) = C(\alpha) \\ c_0\alpha^n &+ c_1\alpha^{n-2} + \quad \cdot + c_{n-2}\alpha + c_{n-1}, \end{aligned}$$

the last member being the canonical form.

If an element of $R(\alpha)$ were expressible in the canonical form in two distinct ways, α would satisfy an equation in R of degree $< n$. Therefore the canonical form is unique.

THEOREM 5. *If α is algebraic relative to R, so is $f(\alpha)$, $f(x)$ being any polynomial in R. If $\alpha_1, \cdots, \alpha_n$ are the conjugates of α relative to R, the conjugates of $f(\alpha)$ relative to R are those of the elements $f(\alpha_1), \cdots, f(\alpha_n)$ that are distinct.*

The coefficients of the polynomial

$$\psi(x) = (x - f(\alpha_1))(x - f(\alpha_2)) \qquad (x - f(\alpha_n))$$

are symmetric functions, with coefficients in R, of $\alpha_1, \alpha_2, \cdots, \alpha_n$, and are therefore elements of R. Since $f(\alpha)$ is a root of the equation $\psi(x) = 0$, $f(\alpha)$ is algebraic relative to R and its degree relative to R is $\leq n$. It follows from Theorem 4 that *every element of $R(\alpha)$ is algebraic relative to R.*

Let $F(x) = 0$ be the primary irreducible equation in R of which $f(\alpha)$ is a root. Since $F[f(\alpha)] = 0$, α is a root of the equation $F[f(x)] = 0$, whose coefficients are elements of R. By Theorem 3 every conjugate of α relative to R is also a root:

$$F[f(\alpha_i)] = 0, \quad (i = 1, \cdots, n).$$

Consequently, $f(\alpha_1), f(\alpha_2), \cdots, f(\alpha_n)$ are roots of the equation $F(x) = 0$, and are therefore conjugates of $f(\alpha)$ relative to R. That $f(\alpha)$ has no other conjugates relative to R follows from Theorem 2 according to which $F(x)$ is a divisor of $\psi(x)$, so that every root of $F(x)$ is a root of $\psi(x)$. The only conjugates of $f(\alpha)$ relative to R are therefore $f(\alpha_1), f(\alpha_2), \cdots, f(\alpha_n)$. But these elements need not be distinct although $\alpha_1, \alpha_2, \cdots, \alpha_n$ are distinct. The conjugates of $f(\alpha)$ relative to R are therefore those of the elements $f(\alpha_1), f(\alpha_2), \cdots, f(\alpha_n)$ that are distinct.

By a suitable choice of the notation we may suppose that $f(\alpha_1), f(\alpha_2), \cdots, f(\alpha_\nu), (\nu \leq n)$ are the distinct conjugates of $f(\alpha)$. The equation

$$F(x) = (x - f(\alpha_1))(x - f(\alpha_2)) \cdots (x - f(\alpha_\nu)) = 0$$

which they satisfy is irreducible in R, and $F(x)$ is a divisor of $\psi(x)$. Let $F(x)$ be a k-fold factor of $\psi(x)$, so that

$$\psi(x) = [F(x)]^k G(x),$$

where $G(x)$ is a polynomial in R which is not divisible by $F(x)$. If $G(x)$ is not a constant it has a root. This root is also a root of $\psi(x)$ and is therefore one of the conjugates of $f(\alpha)$. Since one of the conjugates of $f(\alpha)$ is a root of $G(x)$, $G(x)$ is divisible by $F(x)$ (Theorem 2), contrary to assumption. It follows that $G(x)$ is a constant. This constant must be 1 since $\psi(x)$ and $F(x)$ are primary polynomials. Therefore

$$\psi(x) = [F(x)]^k,$$

so that $n = \nu k$. Thus each of the distinct conjugates of $f(\alpha)$ occurs exactly k times in the set $f(\alpha_1), f(\alpha_2), \cdots, f(\alpha_n)$.

THEOREM 6. *If α is of degree n relative to R, the degree, relative to R, of every element of $R(\alpha)$ is a divisor of n.*

Those elements of $R(\alpha)$ whose degrees relative to $R(\alpha)$ have the maximum value n (the degree of α relative to R) are called *primitive* elements of $R(\alpha)$; all others are called *imprimitive* elements. A primitive element of a field generates the entire field, whereas an imprimitive element generates a subfield. For example, $1 - \sqrt[4]{2}$ and $\sqrt{2} + \sqrt[4]{2}$ are primitive elements of $R(\sqrt[4]{2})$. But $1 + \sqrt{2}$ is an imprimitive element, generating a subfield of degree 2 relative to $R(1)$. Every rational number is also an imprimitive element of

$R(\sqrt[3]{2})$, generating the field $R(1)$ which is of degree 1 relative to $R(1)$.

With the aid of the preceding results it is possible to identify the conjugates of certain algebraic elements without finding the irreducible equations they satisfy.

Example 1. Find the conjugates of $8 - 5\sqrt[3]{2} + 7\sqrt[3]{4}$ relative to $R(1)$.

The conjugates of $\sqrt[3]{2}$ are $\sqrt[3]{2}$, $\omega\sqrt[3]{2}$ and $\omega^2\sqrt[3]{2}$, where ω and ω^2 are the imaginary cube roots of unity. The given number is an element of $R(\sqrt[3]{2})$. Therefore, by Theorem 5, the required conjugates are

$$8 - 5\sqrt[3]{2} + 7\sqrt[3]{4},\ 8 - 5\omega\sqrt[3]{2} + 7\omega^2\sqrt[3]{4},\ 8 - 5\omega^2\sqrt[3]{2} + 7\omega\sqrt[3]{4},$$

which are obviously distinct.

Example 2. Find the conjugates of $\lambda = \sqrt[5]{2 + \sqrt{3}} + \sqrt[5]{2 - \sqrt{3}}$ relative to $R(1)$, the real fifth root being taken in each case.

Since $\sqrt[5]{2 + \sqrt{3}} \cdot \sqrt[5]{2 - \sqrt{3}} = 1$, λ is an element of $R(\alpha)$, where $\alpha = \sqrt[5]{2 + \sqrt{3}}$. In fact, $\lambda = \alpha + \alpha^{-1}$. The 10 conjugates of α relative to $R(1)$ are

$$\epsilon^k\sqrt[5]{2 \pm \sqrt{3}}, \qquad (k = 0, 1, 2, 3, 4),$$

where ϵ is a primitive 5th root of unity. Denoting the conjugates of α by $\alpha_1, \alpha_2, \cdots, \alpha_{10}$, the conjugates of λ are the distinct numbers of the set

$$\alpha_j + \alpha_j^{-1} \qquad (j = 1, \quad, 10).$$

Only five of these numbers are distinct because λ is unaltered when $\sqrt{3}$ and $-\sqrt{3}$ are interchanged. The five distinct conjugates of λ are

$$\epsilon^k\sqrt[5]{2 + \sqrt{3}} + \epsilon^{-k}\sqrt[5]{2 - \sqrt{3}}, \qquad (k = 0, 1, 2, 3, 4).$$

EXERCISES

1. Write the following numbers in the canonical form, the indicated α being a primitive element of the field.

(a) $\dfrac{1 + 2i}{(1 - 2i)^2}$, $\alpha = i$.

(b) same number, $\alpha = 1 - 2i$.

(c) $\dfrac{1 - \sqrt[4]{2}}{1 + \sqrt[4]{2}}$, $\alpha = \sqrt[4]{2}$.

(d) $7 - 4\sqrt{3}$, $\alpha = 5 + 2\sqrt[4]{3}$.

(e) $(3 + 2\sqrt[3]{5})^{-1}$, $\alpha = \sqrt[3]{5}$.

2. Find the conjugates, relative to $R(1)$, of

(a) $-3 + 5\sqrt[3]{3} - 2\sqrt[3]{9}$.

(b) $\sqrt[3]{3 + 2\sqrt{2}} + \sqrt[3]{3 - 2\sqrt{2}}$, the cube roots being real.

(c) $\sqrt[3]{5 + \sqrt{-2}} + \sqrt[3]{5 - \sqrt{-2}}$, the product of the two cube roots being real.

(d) $4 - 7\sqrt[4]{-6} + 2\sqrt{-6} + 9\sqrt[4]{-216}$.

3. Find the conjugates, relative to $R(i)$, of

(a) $\sqrt{3 + 4i}$.

(b) $\sqrt{3 + 4i} - 7\sqrt{3 - 4i}$, where $\sqrt{3 + 4i}\,\sqrt{3 - 4i} \quad +5$.

(c) $\sqrt{-11}$.

(d) $\sqrt{3 + \sqrt{10}} + \sqrt{3 - \sqrt{10}}$, where $\sqrt{3 + \sqrt{10}}\,\sqrt{3 - \sqrt{10}} = +i$.

(e) $6 + 3i + \sqrt{5} - 9i\sqrt{5}$.

4. Find the conjugates, relative to $R(1)$, of each of the numbers of Ex. 3.

5. Find the conjugates, relative to $R(\sqrt{2})$, of

(a) $13 - 8\sqrt{3}$.

(b) $1 - 3\sqrt{2} - 4\sqrt{3} + 7\sqrt{6}$.

(c) $6 - 5\sqrt[4]{2} - 7\sqrt{2} + 3\sqrt[4]{8}$.

(d) $\sqrt{3 + \sqrt{7}} + \sqrt{3 - \sqrt{7}}$, the square roots being positive.

6. Show that $\sqrt{2}$ is not an element of $R(\sqrt[3]{2})$. Generalize. [Apply Theorem 6.]

7. Show that $\sqrt[3]{2}$ is not an element of $R(\sqrt[3]{3})$. [Assume that

$$\sqrt[3]{2} = a + b\sqrt[3]{3} + c\sqrt[3]{9},$$

where a, b, and c are rational numbers, and apply Theorem 5.]

8. Let ϵ be a primitive 7th root of unity. Find the conjugates, relative to $R(1)$, of

(a) $\epsilon + \epsilon^2$. *Ans.* $\epsilon + \epsilon^2$, $\epsilon^2 + \epsilon^4$, $\epsilon^3 + \epsilon^6$, $\epsilon^4 + \epsilon$, $\epsilon^5 + \epsilon^3$, $\epsilon^6 + \epsilon^5$.

(b) $\epsilon + \epsilon^6$. *Ans.* $\epsilon + \epsilon^6$, $\epsilon^2 + \epsilon^5$, $\epsilon^3 + \epsilon^4$.

(c) $\epsilon + \epsilon^2 + \epsilon^4$. *Ans.* $\epsilon + \epsilon^2 + \epsilon^4$, $\epsilon^3 + \epsilon^6 + \epsilon^5$.

(d) $2 - 3\epsilon$.

(e) $\epsilon - \epsilon^2 + \epsilon^4$.

9. Show that if α is a root of the equation $x^3 - 7x + 7 = 0$, the other two roots satisfy the equation $x^2 + \alpha x + \alpha^2 - 7 = 0$. Verify that the other two roots are $-3\alpha^2 - 5\alpha + 14$ and $3\alpha^2 + 4\alpha - 14$.

10. (a) Let α be a root of the equation $x^3 - 7x + 7 = 0$. Express $\beta = \dfrac{4\alpha - 7}{\alpha - 1}$ in the canonical form. *Ans.* $\beta = 3\alpha^2 + 3\alpha - 14$.

(b) Find the primary cubic equation in $R(1)$ which β satisfies.

Ans. $x^3 - 21x - 7 = 0.$

11. Show that if α is a root of the equation

$$x^4 + 2x^3 + 2x^2 + x + 1 = 0,$$

$\alpha + \alpha^2$ is of degree 2 relative to $R(1)$. [Write the equation in the form $(x^2 + x)^2 + x^2 + x + 1 = 0$.]

12. Let $A(x)$ be irreducible in R, and let $B(x)$ be the polynomial whose roots are the mth powers of the roots of $A(x)$. Show that $B(x)$ is reducible in R if, and only if, the ratio of two distinct roots of $A(x)$ is an mth root of unity. [Use Theorem 5.]

58. Multiple algebraic extensions of a field. If α is algebraic relative to R, $R(\alpha)$ is a *simple* algebraic extension of R. If β is algebraic relative to $R(\alpha)$, $R(\alpha, \beta)$ is a simple algebraic extension of $R(\alpha)$, but is a *multiple* algebraic extension of R. Generalizing, $R(\alpha, \beta, \cdots, \lambda)$ is a multiple algebraic extension of R if each of the fields

$$R,\ R(\alpha),\ R(\alpha, \beta),\ \cdots,\ R(\alpha, \beta, \qquad, \lambda)$$

(except the first) is a simple algebraic extension of the preceding field.

A polynomial in the field $R(\alpha)$, where α is algebraic relative to R, may be written in the form

$$(1)\qquad \varphi_0(\alpha)x^s + \varphi_1(\alpha)x^{s-1} + \qquad + \varphi_{s-1}(\alpha)x + \varphi_s(\alpha),$$

where $\varphi_i(\alpha)$ is an element of $R(\alpha)$. Supposing $\varphi_i(\alpha)$ represented in the canonical form (Theorem 4), the function

$$f(x, y) = \varphi_0(y)x^s + \varphi_1(y)x^{s-1} + \cdots + \varphi_{s-1}(y)x + \varphi_s(y)$$

is a polynomial in the independent variables x and y with coefficients in R. The polynomial (**1**) may therefore be written $f(x, \alpha)$, which is a convenient notation for distinguishing polynomials in $R(\alpha)$ from polynomials in R.

THEOREM 7. *If α is algebraic relative to R, and β is algebraic relative to $R(\alpha)$, then β is algebraic relative to R.*

By assumption β is a root of a polynomial $B(x, \alpha) \not\equiv 0$ in $R(\alpha)$. If $\alpha_1, \alpha_2, \cdots, \alpha_n$ are the conjugates of α relative to R, β is also a root of the polynomial

$$B(x, \alpha_1)B(x, \alpha_2) \qquad B(x, \alpha_n) \not\equiv 0,$$

whose coefficients, being symmetric functions of $\alpha_1, \alpha_2, \cdots, \alpha_n$, are elements of R. Since β is a root of a polynomial in R, different from the zero-polynomial, β is algebraic relative to R.

THEOREM 8. If $f(x, \alpha)$ *is a primary irreducible polynomial in* $R(\alpha)$, *and* $\alpha_1, \alpha_2, \cdots, \alpha_n$ *are the conjugates of* α *relative to* R, *then*

$$f(x, \alpha_1)f(x, \alpha_2) \cdots f(x, \alpha_n) = [f(x)]^l, \tag{2}$$

where $f(x)$ *is a primary* **irreducible** *polynomial in* R, *and* l *is a positive integer.*

The left member of (2) is a symmetric function of $\alpha_1, \alpha_2, \cdots, \alpha_n$ and therefore equals a polynomial $E(x)$ with coefficients in R. As $E(x)$ is divisible by $f(x, \alpha)$, we have

$$f(x, \alpha)g(x, \alpha) = E(x),$$

where $g(x, \alpha)$ is a polynomial in $R(\alpha)$ since it is the quotient of the division of $E(x)$ by $f(x, \alpha)$. Since $f(x, \alpha)$ is irreducible in $R(\alpha)$, $f(x, \alpha)$ must be a divisor of some factor of $E(x)$ which is a primary irreducible polynomial in R. Denoting this polynomial by $f(x)$, we have

$$f(x, \alpha)h(x, \alpha) = f(x),$$

where $h(x, \alpha)$ is a polynomial in $R(\alpha)$. This equation (an identity in x) remains valid when α is replaced by any of its conjugates relative to R. We therefore have

$$f(x, \alpha_i)h(x, \alpha_i) = f(x), \qquad (i = 1, \cdots, n).$$

Multiplying these equations, we obtain

$$E(x)Q(x) = [f(x)]^n,$$

where

$$Q(x) = h(x, \alpha_1)h(x, \alpha_2) \cdots h(x, \alpha_n).$$

Since $f(x)$ is irreducible in R, the only primary polynomials in R that are divisors of $[f(x)]^n$ are $1, f(x), [f(x)]^2, \cdots, [f(x)]^n$. Since $E(x)$ is a primary polynomial in R, we conclude that

$$E(x) = [f(x)]^l, \qquad (1 \leq l \leq n).$$

THEOREM 9. (ABEL.) *If* $R(\alpha, \beta, \cdots, \lambda)$ *is a multiple algebraic extension of* R, *there exist elements* $b, \cdots, l$ *of* R *such that*

$$R(\alpha, \beta, \cdots, \lambda) = R(\alpha + b\beta + \cdots + l\lambda).$$

The theorem asserts that the field $R(\alpha, \beta, \cdots, \lambda)$ which, by definition, is generated by several elements, may also be generated by a *single* element. The field therefore contains primitive elements and is algebraic relative to R. As an illustration we shall prove that $R(\sqrt{2}, \sqrt{3}) = R(\sqrt{2} + \sqrt{3})$. It is readily verified that

$$\sqrt{2} = \tfrac{1}{2}[(\sqrt{2} + \sqrt{3})^3 - 9(\sqrt{2} + \sqrt{3})],$$
$$\sqrt{3} = -\tfrac{1}{2}[(\sqrt{2} + \sqrt{3})^3 - 11(\sqrt{2} + \sqrt{3})].$$

Consequently $R(\sqrt{2} + \sqrt{3})$ contains every element of $R(\sqrt{2}, \sqrt{3})$. Conversely, $R(\sqrt{2}, \sqrt{3})$ contains $\sqrt{2} + \sqrt{3}$ and therefore every element of $R(\sqrt{2} + \sqrt{3})$. It follows that $R(\sqrt{2}, \sqrt{3}) = R(\sqrt{2} + \sqrt{3})$.

In proving the theorem it is sufficient to show that $R(\alpha, \beta) = R(\alpha + b\beta)$; for it then follows that $R(\alpha, \beta, \gamma) = R(\alpha + b\beta, \gamma) = R(\alpha + b\beta + c\gamma)$, etc.

Let $\alpha_1 = \alpha, \alpha_2, \cdots, \alpha_n$ be the conjugates of α relative to R and $\beta_1 = \beta, \beta_2, \cdots, \beta_m$ the conjugates of β relative to R (Theorem 7), satisfying the equations $A(x) = 0$ and $B(x) = 0$ respectively, each of which is irreducible in R. The equation

$$\alpha_i + b\beta_j = \alpha_p + b\beta_q, \qquad (i, j \neq p, q)\ *$$

has at most one solution for b. Therefore only a finite number of elements of R exist which satisfy at least one of the equations

$$\alpha_i + b\beta_j = \alpha_p + b\beta_q, \ \begin{pmatrix} i, p = 1, \cdots, n \\ j, q = 1, \cdots, m \end{pmatrix}, \ (i, j \neq p, q).$$

It is therefore possible to choose an element b of R which satisfies none of these equations. We proceed to prove that, for any such choice of b, $R(\alpha, \beta) = R(\alpha + b\beta)$.

First proof: The nm distinct elements $\alpha_i + b\beta_j$ are the roots of the polynomial

$$\begin{aligned} F(x) = {} & (x - \alpha_1 - b\beta_1)(x - \alpha_1 - b\beta_2) \qquad (x - \alpha_1 - b\beta_m) \\ & \times (x - \alpha_2 - b\beta_1)(x - \alpha_2 - b\beta_2) \qquad (x - \alpha_2 - b\beta_m) \\ & \cdots\cdots \\ & \times (x - \alpha_n - b\beta_1)(x - \alpha_n - b\beta_2) \qquad (x - \alpha_n - b\beta_m). \end{aligned}$$

By applying the fundamental theorem on symmetric functions twice we conclude that the coefficients of $F(x)$ are elements of R.

* This statement means that the ordered pair of numbers i, j is not the same as the ordered pair of numbers p, q.

For the coefficients of the polynomial

$$G(x) = (x - b\beta_1)(x - b\beta_2) \cdots (x - b\beta_m)$$

are symmetric functions of $\beta_1, \beta_2, \cdots, \beta_m$, and the coefficients of

$$F(x) = G(x - \alpha_1)G(x - \alpha_2) \cdots G(x - \alpha_n)$$

are symmetric functions of $\alpha_1, \alpha_2, \cdots, \alpha_n$. Now construct by Lagrange's interpolation-formula the unique polynomial $H(x)$ of degree $\leq nm - 1$ such that

$$H(\alpha_i + b\beta_j) = \alpha_i, \qquad \begin{pmatrix} i = 1, \cdots, n \\ j = 1, \cdots, m \end{pmatrix}.$$

This polynomial is

$$H(x) = \alpha_1 \sum_{j=1}^{m} \frac{F(x)}{(x - \alpha_1 - b\beta_j)F'(\alpha_1 + b\beta_j)} + \\ + \alpha_n \sum_{j=1}^{m} \frac{F(x)}{(x - \alpha_n - b\beta_j)F'(\alpha_n + b\beta_j)}.$$

By again applying the fundamental theorem on symmetric functions twice we conclude that the coefficients of $H(x)$ are elements of R. We now have

$$\alpha = H(\tau), \qquad (\tau = \alpha + b\beta = \alpha_1 + b\beta_1),$$

so that α is an element of $R(\tau)$. Since

$$\beta = \frac{\tau - \alpha}{b}, \qquad (b \neq 0),$$

β is also an element of $R(\tau)$. It follows that τ is a primitive element of $R(\alpha, \beta)$.

Second proof: The equations

$$A(\tau - bx) = 0,\ B(x) = 0, \qquad (\tau = \alpha + b\beta)$$

have β as a common root. But they cannot have another root in common; for if β_j $(j \neq 1)$ is a second common root, $\alpha_i = \tau - b\beta_j$ for some $i \leq n$, and $\tau = \alpha + b\beta = \alpha_i + b\beta_j$, contrary to the choice of b. The g.c.d. of $A(\tau - bx)$ and $B(x)$ is therefore a polynomial of the *first* degree in x. This polynomial may be written in the form $x - g(\tau)$, where $g(\tau)$ is an element of $R(\tau)$. Since a common root of two polynomials is a root of their g.c.d., we have

$$\beta = g(\tau), \quad \alpha = \tau - bg(\tau).$$

We conclude that τ is a primitive element of $R(\alpha, \beta)$.

We investigate next the degree of $R(\alpha, \beta)$ relative to R, which is the degree of τ relative to R.

Let β be of degree μ relative to $R(\alpha)$, and let $B(x, \alpha)$ be the primary irreducible polynomial in $R(\alpha)$ which has β as a root. The degree of $B(x, \alpha)$ is μ. By Theorem 8

$$(3) \qquad B(x, \alpha_1)B(x, \alpha_2) \cdots B(x, \alpha_n) = [B(x)]^l,$$

where

$$B(x) = (x - \beta_1)(x - \beta_2) \cdots (x - \beta_m).$$

The roots of the polynomial $B(x, \alpha_i)$ are therefore μ elements of the set $\beta_1, \beta_2, \cdots, \beta_m$. Since $B(x, \alpha)$ is irreducible in $R(\alpha)$, $B(x, \alpha_i)$ is irreducible in $R(\alpha_i)$ by Theorem 3. It follows that the polynomial

$$P(x, \alpha_i) = b^\mu B\left(\frac{x - \alpha_i}{b}, \alpha_i\right)$$

is irreducible in $R(\alpha_i)$, and that its roots are $\alpha_i + b\beta_j$, where j assumes μ distinct values from among the integers $1, \cdots, m$. Because of the conditions imposed upon b no two of the polynomials $P(x, \alpha_1), P(x, \alpha_2), \cdots, P(x, \alpha_n)$ have a root in common. If $P(x)$ is the primary irreducible polynomial in R of which $\tau = \alpha + b\beta$ is a root,

$$P(x, \alpha_1)P(x, \alpha_2) \cdots P(x, \alpha_n) = [P(x)]^l$$

by Theorem 8. Now the left member of this equation is a polynomial which has no multiple root; hence $l = 1$. The degree of $P(x)$, which is also the degree of τ relative to R, is therefore $n\mu$.

THEOREM 10. *If α is of degree n relative to R, and β is of degree μ relative to $R(\alpha)$, then $R(\alpha, \beta)$ is of degree $n\mu$ relative to R.*

EXERCISES

1. Show that if d is the g.c.d. of m and n, the integer of μ Theorem 10 is divisible by m/d. [Apply Theorem 6.]

2. As in the text, let $\beta_1, \beta_2, \cdots, \beta_m$ be the conjugates of β relative to R. Show that if the only common elements of the fields $R(\alpha)$ and $R(\beta_1, \cdots, \beta_m)$ are those of R, then $\mu = m$.

3. Find the degree of

(a) $R(\sqrt{-7}, \sqrt[3]{10})$ relative to $R(1)$. [Apply Ex. 1.]

(b) $R(\sqrt{10}, \sqrt[3]{100}, \sqrt[5]{1000})$ relative to $R(1)$. *Ans.* 30.

(c) $R(\alpha, \beta)$ relative to $R(1)$, where α and β satisfy the equations $x^3 - 2x + 2 = 0$ and $x^5 + 14x - 7 = 0$ respectively.

(d) $R(\sqrt[3]{3}, \sqrt[3]{2})$ relative to $R(1)$. [Show that the equation $x^3 - 2 = 0$ is irreducible in $R(\sqrt[3]{3})$. See Ex. 7, p. 127.]

(e) $R(\sqrt[3]{3}, \sqrt[3]{2})$ relative to $R(\sqrt[3]{6})$. *Ans.* 3.

(f) $R(\sqrt[3]{5}, \sqrt[3]{25})$ relative to $R(1)$.

(g) $R(\sqrt[4]{2}, \sqrt[4]{5})$ relative to $R(1)$. [Apply Ex. 2.]

4. Find the degree, relative to $R(1)$, of

(a) $\sqrt[3]{5} + \sqrt[5]{3}$. [Show that the given number is a primitive element of $R(\sqrt[3]{5}, \sqrt[5]{3})$.]

(b) $\sqrt{1 - \sqrt{2}} + \sqrt{2}$. *Ans.* 4.

(c) $\sqrt{5 - 2\sqrt{3}} + \sqrt[3]{10}$. *Ans.* 12.

(d) $\sqrt[3]{2} + \sqrt[3]{3}$.

5. Prove that the degree, relative to R, of the field generated by the roots of a cubic equation with coefficients in R, is 1, 2, 3, or 6. Find the actual degree in each of the following cases, where $R = R(1)$.

(a) $x^3 - x = 0$. (b) $x^3 + x = 0$. (c) $x^3 = 7$.

(d) $x^3 - 7x + 7 = 0$. [See Ex. 9, p. 127.]

6. Find the degree of the field generated by the roots of the equation

(a) $x^4 = 3$ relative to $R(1)$; relative to $R(i)$; relative to $R(\sqrt{3})$.

Ans. 8; 4; 4.

(b) $x^5 = 4$ relative to $R(1)$; relative to $R(\epsilon)$, where ϵ is a primitive 5th root of unity. *Ans.* 20; 5.

7. Find a polynomial with rational coefficients which is divisible by the polynomial

(a) $x^2 - \sqrt[3]{2}x + 1 + \sqrt[3]{4}$. *Ans.* $x^6 + 3x^4 + 4x^3 + 3x^2 + 6x + 5$.
[Apply the method of the proof of Theorem 7.]

(b) $x^2 + \epsilon x + \epsilon^4$, where ϵ is a primitive 5th root of unity.

Ans. $x^8 - x^7 - 4x^5 + 4x^4 - x^3 - x + 1$.

(c) $x^4 - x^3 + (1 + i)x^2 - (2 + 3i)x - 3 + i$.

8. Let $f(x, \alpha)$ be a polynomial in $R(\alpha)$ and let $\alpha_1, \alpha_2, \cdots, \alpha_n$ be the conjugates of α relative to R. Show that if

$$f(x, \alpha_1) = f(x, \alpha_2) \qquad = f(x, \alpha_n),$$

then $f(x, \alpha)$ is a polynomial in R.

9. (a) In connection with (3), show that $lm = n\mu$.

(b) Solve Exercise 1 with the aid of this result.

(c) Show that β is a primitive element of $R(\alpha, \beta)$ if, and only if, no

two of the polynomials $B(x, \alpha_1)$, $B(x, \alpha_2)$, $\cdots$, $B(x, \alpha_n)$ have a root in common. As an illustration, take $\alpha = \sqrt{2}$, $\beta = \sqrt[4]{2}$, $B(x, \alpha) = x^2 - \alpha$.

10. Show that the integer l of Theorem 8 may have the value 2. [Take $\alpha = \sqrt[3]{2}$, $f(x, \alpha) = x^2 + \alpha x + \alpha^2$.]

11. Let α be a root of the polynomial $A(x)$ irreducible in R. Show that if $x^m - \alpha$ is irreducible in $R(\alpha)$, then $A(x^m)$ is irreducible in R. [Use Theorem 8.]

59. Radicals relative to a field. The equation $x^n = a$ is called a *binomial* equation. Its roots are the nth roots of a, any one of which is denoted by $\sqrt[n]{a}$, which is called a *radical of index* n relative to a field that contains a.

A field R_1 may be extended by successive adjunctions of a root of each of a set of binomial equations

$$x^{n_1} = a_1,\ x^{n_2} = a_2,\ \cdots,\ x^{n_k} = a_k,$$

a_1 being an element of R_1, a_2 of $R_2 = R_1(\sqrt[n_1]{a_1})$, a_3 of $R_3 \quad R_2(\sqrt[n_2]{a_2}) = R_1(\sqrt[n_1]{a_1}, \sqrt[n_2]{a_2})$; etc. The last of these fields is

$$R_k = R_1(\sqrt[n_1]{a_1}, \sqrt[n_2]{a_2}, \cdots, \sqrt[n_k]{a_k}).$$

The elements of R_k are said to be expressible in terms of radicals relative to R_1, being equal to rational functions, with coefficients in R_1, of $\sqrt[n_1]{a_1}$, $\sqrt[n_2]{a_2}$, $\cdots$, $\sqrt[n_k]{a_k}$. Each of these radicals is called a radical relative to R_1.

One of the central problems of the Theory of Equations is that of solving an equation in a field by radicals relative to that field; that is, of expressing the roots of the equation in terms of radicals relative to the field. The reader knows how to solve this problem for quadratic equations and he will presently learn how to do so for cubic and quartic equations.

60. Solution of the general cubic equation by radicals. It is convenient to write the general cubic equation in the form

$$a_0x^3 + 3a_1x^2 + 3a_2x + a_3 = 0, \tag{1}$$

the a's being independent variables. This equation is transformed by the substitution

$$x = \frac{y - a_1}{a_0} \tag{2}$$

into the equation

$$y^3 + 3Hy + G = 0, \tag{3}$$

the sum of whose roots is 0, where

$$G = a_0^2 a_3 - 3a_0 a_1 a_2 + 2a_1^3, \qquad H = a_0 a_2 - a_1^2. \tag{4}$$

It is obvious that if (3) can be solved by radicals, so can (1).

As a result of the experience acquired in determining the degrees of various algebraic elements the reader should have no difficulty in verifying that

(5)

where q and r are independent variables, is of degree 3 relative to the field $R(q, r)$ if

$$p = \sqrt[3]{q + \sqrt{r}}\sqrt[3]{q - \sqrt{r}} \tag{6}$$

is an element of $R(q, r)$. This fact is at the basis of our solution of the general cubic equation.

We now endeavor to express q and r in terms of G and H so that (5) is a root of (3). Denoting (5) by y, we have

$$y^3 = q + \sqrt{r} + 3\sqrt[3]{q + \sqrt{r}}\ \sqrt[3]{q - \sqrt{r}}\left(\sqrt[3]{q + \sqrt{r}} + \sqrt[3]{q - \sqrt{r}}\right) + q - \sqrt{r},$$

which reduces to

$$y^3 - 3py - 2q = 0. \tag{7}$$

In order that (3) and (7) have the same roots it is necessary and sufficient that

$$p = -H, \qquad q = -G/2.$$

By (6), $-H^3 = q^2 - r$. We now have

$$q = -G/2, \qquad r = \tfrac{1}{4}(G^2 + 4H^3).$$

Therefore, by (5),

$$y = -\sqrt[3]{\frac{G}{2} + \frac{1}{2}\sqrt{G^2 + 4H^3}} - \sqrt[3]{\frac{G}{2} - \frac{1}{2}\sqrt{G^2 + 4H^3}} \tag{8}$$

is a root of (3), provided that

$$\sqrt[3]{\frac{G}{2} + \frac{1}{2}\sqrt{G^2 + 4H^3}} \times \sqrt[3]{\frac{G}{2} - \frac{1}{2}\sqrt{G^2 + 4H^3}} = -H. \tag{9}$$

There are three cube roots of $\frac{1}{2}G + \frac{1}{2}\sqrt{G^2 + 4H^3}$ and three cube roots of $\frac{1}{2}G - \frac{1}{2}\sqrt{G^2 + 4H^3}$. Having chosen these cube roots in one way so as to satisfy (**9**), two other choices, indicated by the following equations, may be made:

$$\omega\sqrt[3]{\frac{G}{2} + \frac{1}{2}\sqrt{G^2 + 4H^3}} \times \omega^2\sqrt[3]{\frac{G}{2} - \frac{1}{2}\sqrt{G^2 + 4H^3}} = -H,$$

$$\omega^2\sqrt[3]{\frac{G}{2} + \frac{1}{2}\sqrt{G^2 + 4H^3}} \times \omega\sqrt[3]{\frac{G}{2} - \frac{1}{2}\sqrt{G^2 + 4H^3}} = -H,$$

where ω and ω^2 denote the imaginary cube roots of unity. The conjugates of the right member of (**8**) are thus determined. It follows from (**2**) that the roots of (**1**) are

$$x_1 \quad -\frac{a_1}{a_0} - \frac{1}{a_0}\sqrt[3]{\frac{G}{2} + \frac{1}{2}\sqrt{G^2 + 4H^3}} - \frac{1}{a_0}\sqrt[3]{\frac{G}{2} - \frac{1}{2}\sqrt{G^2 + 4H^3}},$$

$$x_2 = -\frac{a_1}{a_0} - \frac{\omega}{a_0}\sqrt[3]{\frac{G}{2} + \frac{1}{2}\sqrt{G^2 + 4H^3}} - \frac{\omega^2}{a_0}\sqrt[3]{\frac{G}{2} - \frac{1}{2}\sqrt{G^2 + 4H^3}},$$

$$x_3 = -\frac{a_1}{a_0} - \frac{\omega^2}{a_0}\sqrt[3]{\frac{G}{2} + \frac{1}{2}\sqrt{G^2 + 4H^3}} - \frac{\omega}{a_0}\sqrt[3]{\frac{G}{2} - \frac{1}{2}\sqrt{G^2 + 4H^3}}.$$

These expressions for the roots of a cubic equation are known as the *Cardan formulas.*

To solve a given cubic equation by radicals, first calculate G and H by (**4**), then calculate $G^2 + 4H^3$, and apply the Cardan formulas.

EXERCISES

1. Solve the following cubic equations by means of the Cardan formulas.

(a) $x^3 - 24x - 48 = 0$. *Ans.* $x_1 = 2\sqrt[3]{2} + 2\sqrt[3]{4}$.

(b) $x^3 + 3x - 2 = 0$.

(c) $x^3 - 3ix + 1 - i = 0$.

(d) $2x^3 + 3x^2 + 6x - 12 = 0$.

Ans. $x_1 = -\frac{1}{2} - \frac{1}{2}\sqrt[3]{-29 + 2\sqrt{217}} - \frac{1}{2}\sqrt[3]{-29 - 2\sqrt{217}}$.

(e) $x^3 - 3x^2 + 3(1 + \sqrt[3]{2})x + 1 - 3\sqrt[3]{2} = 0$.

Ans. $x_1 = 1 - \sqrt[3]{1 + \sqrt{3}} - \sqrt[3]{1 - \sqrt{3}}$.

2. Express the real root of Exercise 1(d) approximately as a decimal. [Ex. 1(a), p. 93.]

3. Same for Exercise 1(e). *Ans.* .5032.

4. Show that

$$-27(G^2 + 4H^3) = a_0^6(x_1 - x_2)^2(x_2 - x_3)^2(x_3 - x_1)^2.$$

Use the result of Example 1, p. 110, observing that $\sigma_1 = -3a_1/a_0$, $\sigma_2 = 3a_2/a_0$, $\sigma_3 = -a_3/a_0$.

5. Construct a cubic equation with rational coefficients having the indicated number as one root and find the other roots by the method of § 57.

(a) $\sqrt[3]{3} - \sqrt[3]{9}$.

(b) $\sqrt[3]{2 + \sqrt{3}} + \sqrt[3]{2 - \sqrt{3}}$.

(c) $-1 + 2\sqrt[3]{2} - 3\sqrt[3]{4}$.

6. Find the real points of intersection of the curves

$$x^3 + y^3 = 9,\ x^2 - y^2 = 3.$$

Ans. $(2, 1)$, $(c, \frac{1}{2}(c^2 - c))$, where $c = \sqrt[3]{-3 + 2\sqrt{2}} + \sqrt[3]{-3 - 2\sqrt{2}}$.

7. Solve the equation

$$\sqrt[3]{1 + t} + \sqrt[3]{1 - t} = \sqrt[3]{-2}.$$

Ans. $t = \pm \frac{1}{9}\sqrt{-15}$.

8. Find expressions for the dimensions of a rectangular box with a square base in terms of its volume and total area.

9. Let AB be a diameter of a circle, C a point on the tangent line through B, D the point in which the other tangent line through C meets AB produced. Find the radius of the circle, given $AD = 6a$, $BC = 2b$.

61. Trigonometric solution of the irreducible case. The roots of the equation $x^3 - 7x + 7 = 0$ are all real; yet, when they are expressed in terms of radicals by the Cardan formulas they assume the form

$$\begin{aligned}
x_1 &= -\sqrt[3]{\tfrac{7}{2} + \tfrac{7}{18}\sqrt{-3}} - \sqrt[3]{\tfrac{7}{2} - \tfrac{7}{18}\sqrt{-3}},\\
x_2 &= -\omega\sqrt[3]{\tfrac{7}{2} + \tfrac{7}{18}\sqrt{-3}} - \omega^2\sqrt[3]{\tfrac{7}{2} - \tfrac{7}{18}\sqrt{-3}},\\
x_3 &= -\omega^2\sqrt[3]{\tfrac{7}{2} + \tfrac{7}{18}\sqrt{-3}} - \omega\sqrt[3]{\tfrac{7}{2} - \tfrac{7}{18}\sqrt{-3}},
\end{aligned}$$

in which they appear to be imaginary. The explanation of this apparent paradox is quite simple: the two terms of x_1, for example, are conjugate imaginaries, so that their sum is a *real* number.

The cube roots which occur in the Cardan formulas are necessarily imaginary if G and H are real and $G^2 + 4H^3$ is a negative real number. Now a cubic equation with real coefficients for which $G^2 + 4H^3 < 0$ has three distinct, real roots. This statement and its converse follow from the result of Exercise 4, p. 136. Hence, when a cubic which has three distinct real roots is solved by the Cardan formulas, imaginary radicals will necessarily occur. This is known as the *irreducible case.* The problem presented by the

irreducible case is that of obtaining alternative forms of the Cardan formulas which exhibit the roots of a cubic equation in terms of *real* radicals whenever the roots are real. All attempts at solving this problem have proved fruitless; and it is now known that no alternative forms of the Cardan formulas exist.

If the roots of a cubic equation are real and distinct, they can be calculated simultaneously with the aid of a table of cosines. This *trigonometric* solution of the irreducible case is based on the trigonometric identities

$$\begin{aligned} \cos 3\theta &= 4\cos^3\theta - 3\cos\theta \\ &= 4\cos^3(\theta + 120^\circ) - 3\cos(\theta + 120^\circ) \\ &= 4\cos^3(\theta + 240^\circ) - 3\cos(\theta + 240^\circ). \end{aligned} \tag{1}$$

The first of these is a standard formula; the others are obtained from it by replacing θ by $\theta + 120^\circ$ and by $\theta + 240^\circ$ respectively. It follows that the roots of the equation

$$4z^3 - 3z - \cos 3\theta = 0 \tag{2}$$

are $\cos\theta$, $\cos(\theta + 120^\circ)$ and $\cos(\theta + 240^\circ)$.

Now let

$$a_0x^3 + 3a_1x^2 + 3a_2x + a^3 = 0 \tag{3}$$

be a cubic equation which has three real and distinct roots. As in § 60, this equation is transformed by the substitution

$$x = \frac{y - a_1}{a_0} \tag{4}$$

into the equation

$$y^3 + 3Hy + G = 0, \qquad (G^2 + 4H^3 < 0). \tag{5}$$

This equation is transformed by the substitution

$$y = kz \tag{6}$$

into

$$k^3z^3 + 3Hkz + G = 0. \tag{7}$$

We now endeavor to choose k so that (2) and (7) will have the same roots. This will be the case if, and only if, their coefficients are proportional:

$$\frac{3H}{k^2} = -\frac{3}{4}, \qquad \frac{G}{k^3} = -\frac{1}{4}\cos 3\theta, \tag{8}$$

which imply and are implied by

$$(9) \qquad k = 2\sqrt{-H}, \qquad \cos 3\theta =$$

Since $G^2 + 4H^3 < 0$, $G/(2H\sqrt{-H})$ is numerically less than 1. It is therefore possible to find an angle 3θ which satisfies (9).

Either sign of $\sqrt{-H}$ may be chosen. It will be found convenient in practice to choose the sign so that $\cos 3\theta$ is positive. Having found 3θ from a table of cosines, θ, $\theta + 120°$, $\theta + 240°$, and their cosines are readily calculated. We have seen that the roots of (2), which are now also the roots of (7), are $\cos\theta$, $\cos(\theta + 120°)$, and $\cos(\theta + 240°)$. The roots of (5), which are $k = 2\sqrt{-H}$ times the roots of (7), are therefore

$$(10) \quad y_1 = 2\sqrt{-H}\cos\theta, \qquad y_2 = 2\sqrt{-H}\cos(\theta + 120°),$$
$$y_3 = 2\sqrt{-H}\cos(\theta + 240°).$$

Finally, the roots of (3) are, by (4),

$$(11) \qquad x_1 = \frac{y_1 - a_1}{a_0}, \qquad x_2 = \frac{y_2 - a_1}{a_0},$$

As a check, the product of the roots should be calculated by logarithms.

Example. Solve the equation $x^3 + 6x^2 + 6x - 2 = 0$ by the trigonometric method.

Here $a_0 = 1$, $a_1 = 2$, $a_2 = 2$, $a_3 = -2$; $G = 2$, $H = -2$. Since $G^2 + 4H^3$ is negative, the trigonometric method is applicable. Choosing the negative sign of $\sqrt{-H}$,

$$\cos 3\theta = \frac{2}{4\sqrt{2}} = \frac{\sqrt{2}}{4} = .35355.$$

We find from a table of cosines that $3\theta = 69°17.7'$; hence $\theta = 23°5.9'$. By (10)

$$\begin{aligned} y_1 &= -2\sqrt{2}\cos\ 23°5.9' = -2.6017, \\ y_2 &= -2\sqrt{2}\cos 143°5.9' = 2.2618, \\ y_3 &= -2\sqrt{2}\cos 263°5.9' = .3399. \end{aligned}$$

The required roots are, by (11),

$$x_1 = y_1 - 2 = -4.6017, \qquad x_2 = y_2 - 2 = .2618,$$
$$x_3 = y_3 - 2 \quad -1.6601.$$

$$\begin{aligned}
&\log 4.6017 = .66292\\
\textit{Check:}\quad &\log\ .2618 = 9.41797. - 10\\
&\log 1.6601 = .22014\\
&\log 2 \quad\ = .30103.
\end{aligned}$$

EXERCISES

1. Solve the following equations by the trigonometric method.

(a) $x^3 + 6x^2 + 9x + 1 = 0$. *Ans.* $-.1206$, -3.5321, -2.3473.

(b) $x^3 - 9x^2 + 21x - 5 = 0$. *Ans.* $.2680$, 5, 3.7320.

(c) $x^3 + 3x^2 - 6x - 17 = 0$. *Ans.* 2.4114, -3.2266, -2.1848.

(d) $x^3 - 4x^2 + 1 = 0$. *Ans.* 3.9354, $-.4728$, $.5374$.

(e) $x^3 - 30x - 20 = 0$. *Ans.* 5.7841, -5.1072, $-.6770$.

(f) $x^3 - 12x + \sqrt{10} = 0$. *Ans.* -3.5891, 3.3239, $.2651$.

2. Find the length of the base of an isosceles triangle whose perimeter is 12 and whose area is 3. *Ans.* 5.823, 1.107.

3. Find the dimensions of a cylinder inscribed in a sphere of radius 1 if the volume of the cylinder is half that of the sphere.

Ans. radius = .67015, altitude = 1.4845; radius = .91872, altitude = .78986.

4. A rectangular box with a square base has a volume of 30 cu. in., and its altitude exceeds the length of the edge of the base by 6 in. Find the length of the edge of the base. *Ans.* 1.9434.

62. Solution of the general quartic equation by radicals. The general quartic equation

$$a_0x^4 + 4a_1x^3 + 6a_2x^2 + 4a_3x + a_4 = 0, \tag{1}$$

whose coefficients are independent variables, is transformed by the substitution

$$x = \frac{y - a_1}{a_0} \tag{2}$$

into the equation

$$y^4 + 6py^2 + 4qy + r = 0, \tag{3}$$

where

$$\begin{aligned}
p &= a_0a_2 - a_1^2,\\
q &= a_0^2a_3 - 3a_0a_1a_2 + 2a_1^3,\\
r &= a_0^3a_4 - 4a_0^2a_1a_3 + 6a_0a_1^2a_2 - 3a_1^4.
\end{aligned} \tag{4}$$

The following considerations lead to a solution of (**3**). It will be observed that the coefficients of (**3**) involve three independent

variables. To solve this equation we introduce three new variables z_1, z_2, and z_3, in terms of which p, q, and r are to be subsequently expressed, and consider the form of an element which is of degree 4 and is expressed in terms of radicals relative to $R(z_1, z_2, z_3)$. It is evident that $\sqrt{z_1} + \sqrt{z_2}$ is such an element; but, since it involves only two variables, we cannot expect the roots of (3) to be expressible in this form. On the other hand, $\sqrt{z_1} + \sqrt{z_2} + \sqrt{z_3}$ involves the necessary number of variables but is of degree 8 relative to $R(z_1, z_2, z_3)$. Some restriction on the radicals $\sqrt{z_1}$, $\sqrt{z_2}$, and $\sqrt{z_3}$ must be introduced in order to insure that their sum will be of degree 4. The most obvious restriction is that their product be an element of $R(z_1, z_2, z_3)$. We now proceed to the solution of (3). Let

$$y = \sqrt{z_1} + \sqrt{z_2} + \sqrt{z_3}, \tag{5}$$

and let

$$k = \sqrt{z_1}\sqrt{z_2}\sqrt{z_3} \tag{6}$$

be an element of $R(z_1, z_2, z_3)$. We first set up the quartic equation of which y is a root. Squaring

$$y - \sqrt{z_1} = \sqrt{z_2} + \sqrt{z_3},$$

we obtain

$$y^2 - 2y\sqrt{z_1} + z_1 = z_2 + 2\sqrt{z_2}\,\sqrt{z_3} + z_3.$$

Transposing, and squaring

$$y^2 + z_1 - z_2 - z_3 = 2y\sqrt{z_1} + 2\sqrt{z_2}\,\sqrt{z_3},$$

we obtain

$$y^4 + 2(z_1 - z_2 - z_3)y^2 + z_1^2 + z_2^2 + z_3^2 - 2z_1z_2 - 2z_1z_3 + 2z_2z_3 \\ = 4z_1y^2 + 8ky + 4z_2z_3,$$

where k is given by (6). Hence

$$y^4 - 2(z_1 + z_2 + z_3)y^2 - 8ky + z_1^2 + z_2^2 + z_3^2 - 2z_1z_2 - 2z_1z_3 \\ - 2z_2z_3 = 0.$$

This equation reduces to

$$y^4 - 2\sigma_1y^2 - 8ky + \sigma_1^2 - 4\sigma_2 = 0, \tag{7}$$

where

$$\sigma_1 = z_1 + z_2 + z_3, \qquad \sigma_2 = z_1z_2 + z_2z_3 + z_3z_1.$$

The same quartic equation (7) is obtained from (5) no matter which signs of $\sqrt{z_1}$, $\sqrt{z_2}$, and $\sqrt{z_3}$ are chosen, provided that (6) is verified. As there are four choices of the signs which verify (6), all four roots of (7) are known.

We now endeavor to choose k, σ_1, and σ_2 so that (7) and (3) are identical. Necessary and sufficient conditions are

$$(8) \qquad \sigma_1 = -3p, \qquad k = -\tfrac{1}{2}q, \qquad \sigma_1^2 - 4\sigma_2 = r.$$

From these equations and (6) we readily deduce that

$$(9) \qquad \sigma_1 = -3p, \qquad \sigma_2 = \tfrac{1}{4}(9p^2 - r), \qquad \sigma_3 = z_1z_2z_3 = \tfrac{1}{4}q^2.$$

Therefore z_1, z_2, and z_3 are the roots of the *resolvent cubic equation*

$$(10) \qquad z^3 + 3pz^2 + \tfrac{1}{4}(9p^2 - r)z - \tfrac{1}{4}q^2 = 0.$$

It is found convenient to transform this equation by the substitution

$$(11) \qquad z = \tfrac{1}{2}a_0u - p$$

into *Euler's resolvent cubic*

$$(12) \qquad u^3 - g_2u + 2g_3 = 0,$$

where

$$(13) \qquad g_2 = \frac{3p^2 + r}{a_0^2}, \qquad g_3 - \frac{-p^3 + pr - q^2}{a_0^3}$$

By means of (4), g_2 and g_3 may be expressed directly in terms of the a's. We find that

$$(14) \qquad g_2 = a_0a_4 - 4a_1a_3 + 3a_2^2,$$

$$(15) \qquad g_3 = a_0a_2a_4 - a_0a_3^2 + 2a_1a_2a_3 - a_1^2a_4 - a_2^3.$$

The roots of (12) may be expressed in terms of radicals by means of the Cardan formulas. Denoting these roots by u_1, u_2, and u_3, the roots of (10) are, by (11),

$$z_i = \tfrac{1}{2}a_0u_i - p = \tfrac{1}{2}a_0u_i - a_0a_2 + a_1^2, \qquad (i = 1, 2, 3).$$

It follows from (5) and (2) that the roots of (1) are

$$(16) \qquad -\frac{a_1}{a_0} + \frac{\pm}{a_0}\sqrt{\tfrac{1}{2}a_0u_1 - a_0a_2 + a_1^2} + \frac{\pm}{a_0}\sqrt{\tfrac{1}{2}a_0u_2 - a_0a_2 + a_1^2}$$
$$+ \frac{1}{a_0}\sqrt{\tfrac{1}{2}a_0u_3 - a_0a_2 + a_1^2},$$

the four possible combinations of signs of the square roots being chosen so that their product equals

$$-\tfrac{1}{2}(a_0{}^2a_3 - 3a_0a_1a_2 + 2a_1{}^3), \tag{17}$$

which is the value of k by (8) and (4).

Example. Solve the equation $x^4 + 4x^3 - 24x - 24 = 0$.

Here $a_0 = 1$, $a_1 = 1$, $a_2 = 0$, $a_3 = -6$, $a_4 = -24$. We find that $g_2 = 0$, $g_3 = -12$, $k = 2$, $a_1{}^2 - a_0a_2 = 1$. The resolvent cubic is $u^3 - 24 = 0$, whose roots are

$$u_1 = 2\sqrt[3]{3}, \qquad u_2 = 2\omega\sqrt[3]{3}, \qquad u_3 = 2\omega^2\sqrt[3]{3},$$

where ω and ω^2 are the imaginary cube roots of unity. Suitable signs must now be assigned to

$$\sqrt{1+\sqrt[3]{3}}, \qquad \sqrt{1+\omega\sqrt[3]{3}}, \qquad \sqrt{1+\omega^2\sqrt[3]{3}},$$

so that their product equals $k = +2$. Let us agree that $\sqrt[3]{3}$ represents the real cube root of 3 and that $\sqrt{1+\sqrt[3]{3}}$ is the positive square root of $1 + \sqrt[3]{3}$. Let the signs of the other two square roots be chosen so that their product, which equals the *real* number $\sqrt{1 - \sqrt[3]{3} + \sqrt[3]{9}}$, is positive. Since the product of the three square roots is positive, as required, the four roots are

$$\begin{aligned}
x_1 &= -1 + \sqrt{1+\sqrt[3]{3}} + \sqrt{1+\omega\sqrt[3]{3}} + \sqrt{1+\omega^2\sqrt[3]{3}},\\
x_2 &= -1 + \sqrt{1+\sqrt[3]{3}} - \sqrt{1+\omega\sqrt[3]{3}} - \sqrt{1+\omega^2\sqrt[3]{3}},\\
x_3 &= -1 - \sqrt{1+\sqrt[3]{3}} + \sqrt{1+\omega\sqrt[3]{3}} - \sqrt{1+\omega^2\sqrt[3]{3}},\\
x_4 &= -1 - \sqrt{1+\sqrt[3]{3}} - \sqrt{1+\omega\sqrt[3]{3}} + \sqrt{1+\omega^2\sqrt[3]{3}}.
\end{aligned}$$

EXERCISES

1. Solve the following equations by radicals. If the resolvent cubic has rational coefficients, examine it for rational roots before applying the Cardan formulas.

(a) $x^4 + 4x^3 + 8x + 8 = 0$.

Ans. $x_1 = -1 - \sqrt{1+\sqrt[3]{3}} + \sqrt{1+\omega\sqrt[3]{3}} + \sqrt{1+\omega^2\sqrt[3]{3}}$.

(Compare with the illustrative example.)

(b) $x^4 + 8x^3 + 42x^2 - 8x + 281 = 0$.

Ans. $x_1 = -2 + \sqrt{7} + i\sqrt{2} - i\sqrt{14}$.

(c) $x^4 + 6x^2 - 4x + 2 = 0$.

$$Ans.\ x_1 = -i + \sqrt{\tfrac{1}{2}\sqrt{5} - 1} + i\sqrt{\tfrac{1}{2}\sqrt{5} + 1}.$$

(d) $4x^4 - 12x^2 + 12x - 5 = 0$. *Ans.* $\frac{1}{2}(1 \pm i), \frac{1}{2}(-1 \pm \sqrt{11})$.
[Observe that $10 \pm 2i\sqrt{11} = (i \pm \sqrt{11})^2$.]

(e) $x^4 - 8\sqrt{6}x + 24 = 0$.

$$Ans.\ x_1 = \sqrt{\sqrt[3]{2} + \sqrt[3]{4}} + \sqrt{\omega\sqrt[3]{2} + \omega^2\sqrt[3]{4}} + \sqrt{\omega^2\sqrt[3]{2} + \omega\sqrt[3]{4}}.$$

(f) $x^4 + 4ix^3 - 1 = 0$.

2. Verify that g_3 $\begin{vmatrix} a_0 & a_1 & a_2 \\ a_1 & a_2 & a_3 \\ a_2 & a_3 & a_4 \end{vmatrix}$

3. Find the roots of the equation $x^4 - 8x + 12 = 0$ by solving the resolvent cubic by the trigonometric method.

Ans. $1.3709 \pm .6484i, -1.3709 \pm 1.8270i$.

4. Construct a quartic equation with rational coefficients having one root equal to $\sqrt{2} + \sqrt{3} + \sqrt{6}$. What are the other roots?

5. Construct a quartic equation with rational coefficients having one root equal to

$$\sqrt{3\sqrt[3]{3} - 2\sqrt[3]{9}} + \sqrt{3\omega\sqrt[3]{3} - 2\omega^2\sqrt[3]{9}} + \sqrt{3\omega^2\sqrt[3]{3} - 2\omega\sqrt[3]{9}},$$

the signs of the square roots being chosen so that their product is positive.

Ans. $y^4 - 24y - 216 = 0$.

6. Construct a quartic equation in the field $R(\sqrt{\cos 3\theta})$ having one root equal to

$$\sqrt{\cos\theta} + \sqrt{\cos(\theta + 120°)} + \sqrt{\cos(\theta + 240°)}.$$

Ans. $y^4 \pm 4\sqrt{\cos 3\theta}\, y + 3 = 0$.

CHAPTER VIII

ALGEBRAICALLY CLOSED FIELDS

63. Introduction. A field is said to be *algebraically closed* if every non-constant polynomial in the field has a root in the field. It is easy to prove that the defining property of an algebraically closed field implies and is implied by each of the following properties: (a) Every polynomial in the field of degree ≥ 2 is reducible in the field. (b) Every non-constant polynomial in the field equals the product of linear polynomials in the field. Any one of these three properties may therefore be chosen as the defining property of an algebraically closed field.

This chapter is devoted to algebraically closed fields. We shall prove in the next section that the field of complex numbers is algebraically closed, a theorem which is known as the Fundamental Theorem of Algebra. But the field of complex numbers is not the only algebraically closed field, and we shall call attention to other such fields.

64. Proof of the Fundamental Theorem of Algebra. The proof which follows is a modification of Gordan's proof, by mathematical induction, of the Fundamental Theorem of Algebra.* The basic idea of the proof consists in showing that if, for a fixed k, every polynomial whose degree is not divisible by 2^k has a root, then every polynomial whose degree has the form $2^k m$ (m odd) has a root. The proof is almost entirely algebraic. The only non-algebraic part of the proof is that in which use is made of the theorem that every polynomial of odd degree with real coefficients has at least one real root, whose proof (§ 32) involves the non-algebraic concept of continuity. For convenience the proof is divided into several parts.

THEOREM 1. *If $A(x)$ is a polynomial of degree $n \geq 2$ in a field R, there exist polynomials $U(x, y)$, $V(x, y)$ and $F(y)$ in R such that*

$$(1) \qquad A(x + y/2)U(x, y) + A(-x + y/2)V(x, y) = A(y/2)\,[F(y)]^2,$$

the degree of $F(y)$ being $\frac{1}{2}n(n-1)$.

* For Gordan's proof see H. Weber, *Kleines Lehrbuch der Algebra* (1912), p. 109.

Let $x_1, \cdots, x_n$ be n independent variables and $\sigma_1, \cdots, \sigma_n$ their elementary symmetric functions, so that

$$f(x) = (x - x_1) \cdots (x - x_n) = x^n - \sigma_1 x^{n-1} + \cdots + (-1)^n \sigma_n.$$

The roots of the equation $f(-x + y/2) = 0$, regarded as an equation in x, are $y/2 - x_1, \cdots, y/2 - x_n$; and the roots of the equation $f(x + y/2) = 0$ are $x_1 - y/2, \cdots, x_n - y/2$. The resultant of $f(-x + y/2)$ and $f(x + y/2)$ is therefore (§ 45)

$$(2) \qquad \rho[f(-x + y/2), f(x + y/2)] = \prod_{i,j=1}^{n} (y - x_i - x_j).$$

The right member equals a polynomial in y whose coefficients are symmetric functions of $x_1, \cdots, x_n$. Hence

$$(3) \qquad \rho[f(-x + y/2), f(x + y/2)] = P(y, \sigma_1, \cdots, \sigma_n),$$

where P is a polynomial in its arguments, with integral coefficients. This polynomial can be factored. For if, in the right member of (2), we collect those factors in which $i = j$, we have

$$(4) \qquad \prod_{i=1}^{n}(y - 2x_i) = 2^n \prod_{i=1}^{n} (y/2 - x_i) = 2^n f(y/2).$$

Since i and j range independently over all integers from 1 to n inclusive in (2), each of the remaining factors of (2) occurs twice. Hence

$$(5) \qquad P(y, \sigma_1, \cdots, \sigma_n) = 2^n f(y/2)[F(y, \sigma_1, \cdots, \sigma_n)]^2,$$

where

$$(6) \qquad F(y, \sigma_1, \cdots, \sigma_n) = \prod_{1 \leqq i < j \leqq n} (y - x_i - x_j).$$

As indicated by the notation, F is a polynomial in y whose coefficients are symmetric functions of $x_1, \cdots, x_n$. The degree of F in y is clearly $\frac{1}{2}n(n - 1)$.

By § 43 polynomials $U = U(x, y, \sigma_1, \cdots, \sigma_n)$ and $V = V(x, y, \sigma_1, \cdots, \sigma_n)$ exist such that

$$(7) \quad f(x + y/2)U + f(-x + y/2)V = 2^n f(y/2)[F(y, \sigma_1, \cdots, \sigma_n)]^2.$$

This is an identity in $x, y, x_1, \cdots, x_n$ if $\sigma_1, \cdots, \sigma_n$ are thought of as functions of $x_1, \cdots, x_n$. Now wherever $x_1, \cdots, x_n$ occur in (7) they occur as combinations of symmetric functions of these

variables. When these symmetric functions are expressed in terms of the elementary symmetric functions (7) becomes an identity in $x, y, \sigma_1, \cdots, \sigma_n$, since the σ's are functionally independent (§ 48). Therefore (7) becomes an identity in x and y when particular values (elements of a field) are assigned to the σ's without cognizance being taken of $x_1, \cdots, x_n$.

Now let

$$A(x) = a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n, \qquad (a_0 \neq 0)$$

be a polynomial in a field R. In (7) substitute

$$\sigma_1 = -a_1/a_0,\ \sigma_2 = a_2/a_0,\ \cdots,\ \sigma_n = (-1)^n a_n/a_0.$$

Then $f(x) = A(x)/a_0$. After dividing by a constant, which may be absorbed in the U and the V, (7) yields (1). It must be emphasized that in thus establishing (1) we have not assumed the existence of a root of the polynomial $A(x)$.

The conjugate imaginary of a complex number c will be denoted by $\bar{c}$. If

$$C(x) = c_0x^m + c_1x^{m-1} + \cdots + c_{m-1}x + c_m$$

is a polynomial in the field of complex numbers, $\overline{C}(x)$ is defined by

$$\overline{C}(x) = \bar{c}_0x^m + \bar{c}_1x^{m-1} + \cdots + \bar{c}_{m-1}x + \bar{c}_m.$$

LEMMA 1. *Every polynomial of odd degree > 1 in the field of complex numbers is reducible in that field.*

Let $B(x)$ be a primary polynomial of odd degree $m > 1$ in the field of complex numbers, and suppose that $B(x)$ is irreducible in that field. $\overline{B}(x) \neq B(x)$; in the contrary case the coefficients of $B(x)$ would be real and $B(x)$ would have a real root. Construct the polynomial $A(x) = B(x)\overline{B}(x)$ of degree $n = 2m$ with real coefficients. By Theorem 8, p. 129, $A(x) = [P(x)]^l$, where $P(x)$ is a polynomial which is irreducible in the field of real numbers. If l were ≥ 2, $A(x)$ would have a repeated factor which is clearly not the case. Therefore $A(x)$ is irreducible in the field of real numbers.

To this polynomial $A(x)$ we now apply Theorem 1. The corresponding polynomial $F(y)$ is of degree $\frac{1}{2}n(n-1) = m(2m-1)$, an *odd* number. Since the coefficients of $F(y)$ are real, this polynomial has a real root y_0. It follows from (1) that the polynomials $A(x + y_0/2)$ and $A(-x + y_0/2)$ are not relatively prime. Since

these polynomials have the same leading coefficient, and since $A(x)$ is irreducible in the field of real numbers,

$$A(x + y_0/2) = A(-x + y_0/2);$$

from which we infer that when $A(x + y_0/2)$ is expressed in powers of x, no odd powers occur. Hence

$$A(x + y_0/2) = g(x^2),$$

where $g(x)$ is a polynomial with real coefficients. The polynomial $g(x)$, being of odd degree m, has a real root γ. It follows that

$$\alpha = \sqrt{\gamma} + y_0/2$$

(a real or an imaginary number according as $\gamma \geq 0$ or $\gamma < 0$) is a root of $A(x)$; for

$$A(\alpha) = A(\sqrt{\gamma} + y_0/2) = g(\gamma) = 0.$$

Since $B(\alpha)\overline{B}(\alpha) = 0$, either $B(\alpha) = 0$ or $\overline{B}(\alpha) = 0$. If $B(\alpha) = 0$, $B(x)$ is divisible by $x - \alpha$. If $\overline{B}(\alpha) = 0$, then $B(\overline{\alpha}) = 0$, and $B(x)$ is divisible by $x - \overline{\alpha}$.

LEMMA 2. *Every polynomial of odd degree in the field of complex numbers has a root in that field.*

If $B(x)$ is a polynomial of odd degree > 1 in the field of complex numbers, $B(x)$ is reducible by Lemma 1: $B(x) = B_1(x)B_2(x)$. One of the polynomials $B_1(x)$ and $B_2(x)$ must be of odd degree and the other of even degree. If $B_1(x)$ is of odd degree > 1, $B_1(x)$ is reducible. By repeating this argument we conclude that $B(x)$ has a linear factor, and hence a root, in the field of complex numbers.

LEMMA 3. *If, for a certain $k \geq 1$, every polynomial in the field of complex numbers whose degree is not divisible by 2^k has a root, then every polynomial in the field of complex numbers whose degree is divisible by 2^k but not by 2^{k+1} has a root.*

Let $A(x)$ be a polynomial of degree $n = 2^k m$, where m is an odd number. The degree of the corresponding polynomial $F(y)$ of Theorem 1 is $2^{k-1}m(2^k m - 1)$, which is divisible by 2^{k-1} but not by 2^k. It follows from our hypothesis that $F(y)$ has a root y_0 (a complex number). Hence $A(x + y_0/2)$ and $A(-x + y_0/2)$ have a non-constant common factor.

Suppose first that these two polynomials are equal. As in the proof of Lemma 1,

$$A(x + y_0/2) = g(x^2),$$

where $g(x)$ is a polynomial of degree $n/2 = 2^{k-1}m$ and therefore has a root γ (which need not be a real number as in the proof of Lemma 1). It follows that $A(x)$ has the root $\sqrt{\gamma} + y_0/2$.

If $A(x + y_0/2) \neq A(-x + y_0/2)$, $A(x)$ is reducible in the field of complex numbers: $A(x) = A_1(x)P_1(x)$. Let $n_1 \geq 1$ and $p_1 \geq 1$ be the degrees of $A_1(x)$ and $P_1(x)$ respectively. Since $2^k m = n_1 + p_1$, at least one of the integers n_1 and p_1 is not divisible by 2^{k+1}; let n_1 be not divisible by 2^{k+1}. If n_1 is not divisible by 2^k, $A_1(x)$ has a root by hypothesis. If n_1 is divisible by 2^k, the preceding argument is applied to $A_1(x)$. Then, either $A_1(x)$ has a root, or else a divisor whose degree $n_2 < n_1$ is divisible by 2^k but not by 2^{k+1}. Continuing thus we obtain a sequence of decreasing positive integers $n, n_1, n_2, \cdots$, all divisible by 2^k but not by 2^{k+1}. As this sequence cannot consist of an infinite number of numbers, we must finally arrive at a divisor of $A(x)$ which has a root. This root is also a root of $A(x)$.

THEOREM 2. *The field of complex numbers is algebraically closed.*

Since every polynomial of odd degree has a root by Lemma 2, every polynomial whose degree is twice an odd number has a root by Lemma 3. Applying Lemma 3 again we infer that every polynomial whose degree is four times an odd number has a root. Continuing thus we conclude that every polynomial in the field of complex numbers has a root in that field.

EXERCISES

1. Show that each of the three properties of an algebraically closed field implies the other two.

2. Show that a polynomial of degree n in an algebraically closed field has exactly n roots in the field, each root being counted to its degree of multiplicity.

3. Calculate the $F(y)$ of Theorem 1 corresponding to

$$A(x) = x^3 + a_1x^2 + a_2x + a_3.$$

$$\textit{Ans.}\ F(y) = y^3 + 2a_1y^2 + (a_1^2 + a_2)y + a_1a_2 - a_3.$$

4. Show that if a root of the equation

$$a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n = 0$$

in the field of complex numbers is $\leq P$ in absolute value ($P > 0$), then

$$|a_n| \leq |a_0|P^n + |a_1|P^{n-1} + \cdots + |a_{n-1}|P.$$

5. Show that if a root of the equation of Ex. 4 is $\geq Q > 0$ in absolute value, then

$$|a_0| Q^n \leq |a_1| Q^{n-1} + |a_2| Q^{n-2} + \cdots + |a_{n-1}| Q + |a_n|.$$

Hence if $M > 0$ satisfies the inequality

$$|a_0| M^n \geq |a_1| M^{n-1} + |a_2| M^{n-2} + \cdots + |a_{n-1}| M + |a_n|,$$

the absolute value of every root of the equation is $\leq M$.

6. Use the preceding result to find a positive integer which exceeds the absolute value of every root of the equation

(a) $x^4 + 20x^3 - 9x^2 + x + 13 = 0$.

(b) $8x^5 + 7x^4 - 10x^3 + 6x^2 - 7x - 11 = 0$.

(c) $x^3 + (\sqrt{2} + 3i)x^2 + (-3 - i)x - 4 + i\sqrt{2} = 0$.

(d) $x^4 + (6 - 2\sqrt{5})x^2 + (-2 + 5\sqrt{5})x + 9 - \sqrt{5} = 0$.

(e) $x^n - x + 1 = 0$.

(f) $x^n - x^{n-1} - x^{n-2} - \cdots - x - 1 = 0$.

7. Find the real roots (if any) of the polynomial

$$A(x) = x^5 + 2x^4 + ix^3 + 2x^2 + (-1 - 5i)x + 2i.$$

[Find the g.c.d. of $A(x)$ and $\bar{A}(x)$.]

8. The equation $x^4 + (1 - i)x^3 + 3ix^2 + (1 - 3i)x + 1 + 2i = 0$ has a pair of conjugate imaginary roots. Find them.

65. Other algebraically closed fields. The following theorem points to the existence of algebraically closed number-fields different from the field of complex numbers.

THEOREM 3. *The complex numbers which are algebraic relative to a given number-field form an algebraically closed field.*

Let α and β be two algebraic elements relative to a number-field R; and let α and β be roots of the polynomials $A(x)$ and $B(x)$ respectively with coefficients in R, where $A(x)B(x) \neq 0$. Let y be a new variable, and let $G(y)$ be the resultant with respect to x of the polynomials

$$A(y - x) \text{ and } B(x). \tag{1}$$

Substituting $y = \alpha + \beta$ in (1), we have two polynomials $A(\alpha + \beta - x)$ and $B(x)$ which have β as a common root. Therefore $G(\alpha + \beta) = 0$. Since $G(y) \neq 0$ is a polynomial in R, $\alpha + \beta$ is algebraic relative to R. In a similar manner let the reader show that $\alpha - \beta$, $\alpha\beta$, and α/β ($\beta \neq 0$) are algebraic relative to R, being roots of the resultant with respect to x of

$$A(y + x) \text{ and } B(x), \tag{2}$$

$$x^n A(y/x) \text{ and } B(x), \tag{3}$$

$$A(xy) \text{ and } B(x), \tag{4}$$

respectively. In (**3**) the factor x^n, where n is the degree of $A(x)$, is introduced to secure a *polynomial.* We conclude that the sum, difference, product, and quotient of any two complex numbers which are algebraic relative to R are algebraic relative to R. Therefore the algebraic elements relative to R form a field R'. We proceed to prove that R' is algebraically closed.

Let

$$C(x) = c_0x^h + c_1x^{h-1} + \qquad + c_{h-1}x + c_h$$

be a polynomial in R'. The field $R(c_0, c_1, \cdots, c_h)$ is algebraic relative to R and contains a primitive element τ (Theorem 9, p. 129); and

$$c_i = \varphi_i(\tau), \qquad (i = 0, 1, \qquad, h),$$

where $\varphi_i(x)$ is a polynomial in R (Theorem 4, p. 123). Let $\tau_1, \cdots,$ τ_k be the conjugates of τ relative to R. Construct the polynomials

$$C_i(x) = \varphi_0(\tau_i)x^h + \varphi_1(\tau_i)x^{h-1} + \qquad + \varphi_{h-1}(\tau_i)x + \varphi_h(\tau_i), \quad (i = 0, 1, \cdots, k),$$

among which $C(x)$ is included. Their product

$$H(x) = C_1(x)C_2(x) \cdots C_k(x)$$

is a polynomial in R, as its coefficients are symmetric functions of $\tau_1, \cdots, \tau_k$. Therefore, by the definition of R', all the roots of $H(x)$ are elements of R'. Since the roots of $C(x)$ are included among those of $H(x)$, the roots of $C(x)$ are elements of R'. Now $C(x)$ was selected as *any* polynomial in R'. Hence the roots of *every* polynomial in R' are elements of R', and R' is algebraically closed.

An algebraic number (p. 119) is a complex number which is algebraic relative to the field of rational numbers. As a consequence of Theorem 3, *the algebraic numbers form an algebraically closed field.* This is the smallest algebraically closed field which contains the rational numbers.

It is known that there are complex numbers which are not

algebraic numbers. Such numbers are called *transcendental numbers.** Examples of transcendental numbers are the familiar numbers $e = 2.781828 \cdots$ and $\pi = 3.14159 \cdots$.†

Although the number of algebraic numbers is infinite, as well as the number of transcendental numbers, there are "more" transcendental numbers than algebraic numbers in a certain sense which is defined in works on the Theory of Aggregates which we shall not undertake to describe here. With the aid of elementary theorems on the cardinal numbers of infinite sets we shall prove that *the field of complex numbers contains an infinite number of algebraically closed fields.*

Let R_0 be the field of algebraic numbers and τ_1 a transcendental number. The complex numbers which are algebraic relative to $R_0(\tau_1)$ form an algebraically closed field R_1 by Theorem 3. Let τ_2 be a complex number not contained in R_1. The complex numbers which are algebraic relative to $R_1(\tau_2)$ form an algebraically closed field R_2. Continuing thus we obtain a sequence of algebraically closed fields $R_0, R_1, R_2, \cdots$, each of which is a subfield of its successors. The results of the Theory of Aggregates to which we have alluded assure us that this sequence may be continued indefinitely. The field of complex numbers therefore contains an infinite number of algebraically closed fields.

The preceding discussion gives one an insight into the highly complicated structure of the field of complex numbers from the algebraic point of view. It shows that the field of complex numbers cannot be obtained from the field of rational numbers by algebraic operations. On the other hand, the notion of a *limit* (a concept which belongs to Analysis rather than to Algebra) does provide a method for constructing the field of complex numbers: the field of real numbers is obtained at one swoop by adjoining to the field of rational numbers all limits of convergent sequences of rational numbers, and the field of complex numbers is then obtained by adjoining i to the field of real numbers.

We also infer from the preceding results that the field of complex numbers is not created for the purpose of securing an alge-

* In 1840 Liouville proved a theorem which enabled him to prove the existence of transcendental numbers. On Liouville's theorem the reader may consult G. H. Hardy, *An Introduction to the Theory of Numbers*, Bulletin of the American Mathematical Society, Vol. 35 (1929), p. 789; E. Landau, *Vorlesungen über Zahlentheorie* (1927), Vol. 3, p. 38 and p. 91.

† For proofs see Landau, *loc. cit.*, pp. 92 ff.

braically closed field which contains the field of rational numbers, as is occasionally asserted. For that purpose it would be sufficient to create merely the field of algebraic numbers. The field of complex numbers has a property which is not shared by any of its algebraically closed subfields: it is *compact;* that is, every convergent sequence of complex numbers has a limit which is a complex number. The field of complex numbers is the smallest field containing the field of rational numbers which is both compact and algebraically closed. It is the possession of both of these properties which accounts for the important rôle which the field of complex numbers plays in mathematics.

CHAPTER IX

CONSTRUCTIONS BY RULER AND COMPASSES

66. Introduction. Among the problems considered in elementary geometry there is a large number of the following type: Given a certain configuration consisting of points, lines, line-segments, angles, and circles (called *geometric elements*), to construct one or more geometric elements having a stated property or a certain relation to the given configuration. It is demanded that only ruler and compasses be employed in the construction. In this chapter we shall develop methods of determining whether or not a proposed construction is possible with ruler and compasses.

It is important to understand precisely what the nature of the proposed problem is and what means it is permissible to employ in the solution of the problem. Certain points, lines, etc., are "given"; that is, they are assumed to have been drawn in a plane. No relations are to be assumed among the given elements other than those asserted in the statement of the problem. If the problem is concerned with two given parallel lines, then, of course, the fact that these lines are parallel may be used in the course of the solution of the problem. But if the problem merely states "given two lines $\cdots$," and no relation between them is mentioned, the lines may not be assumed to be parallel or perpendicular or to have any other special relation. Again, if two or more line-segments are given, and no relation among them is mentioned, we may not assume that the lengths or the ratios of the lengths of these lines are known as fixed real numbers. To be sure, we may introduce symbols to represent their lengths or the ratios of their lengths, but these symbols are to be regarded as *parameters* and not as known real numbers; they are *real* parameters since they assume only real values.

The fundamental constructions are:

1. Joining two points by a line-segment.
2. Drawing an infinite line through two points.
3. Drawing a circle with a given point as center and a given line-segment as radius.

The first two constructions are effected by a ruler and the third by compasses.

All other constructions consist of two or more applications of these fundamental constructions.

Being given certain geometric elements, new elements may be found. A line-segment, as well as a line, is determined by two given points. New points are determined by the intersection of given lines, lines and circles, or circles. These new elements may be employed to find other elements; etc. The fundamental constructions may be employed *any finite number of times* for the purpose of solving a given problem. Moreover, it is permissible to introduce any other geometric element provided that it is not assumed that this element has a special relation to the given elements, unless the possibility of constructing this special element has been previously demonstrated. It is permissible, for example, to draw an *arbitrary* line through a given point, or to draw a circle of *arbitrary* radius with a given point as center; but it is not permissible to prescribe that a line is to be drawn through a given point making some special angle, such as 62°, with a given line, or that a circle is to be drawn with a given point as center and having a radius equal to $\sqrt[3]{2}$.

The reader who wishes to understand the pitfalls into which circle-squarers and angle-trisectors have fallen will do well to reconsider the preceding remarks, as ignorance of the nature of the problem to be solved and of the means which it is permissible to employ in the solution of the problem are largely responsible for the so-called solutions of the problems of squaring the circle and trisecting the angle which are occasionally heralded by the press.

67. The field $R^{\frac{1}{2}}$ relative to R. Let $R^{\frac{1}{2}}$ denote the set of all algebraic elements relative to a field R which are expressible in terms of radicals of index 2 (square roots) relative to R (§ 59). A typical element of $R^{\frac{1}{2}}$ consists of the sum of a finite number of terms of the form

$$(1) \qquad g_1\sqrt{h_1 + g_2\sqrt{h_2 + g_3\sqrt{\cdots + g_k\sqrt{h_k}}}},$$

where k is a positive integer and the g's and h's are elements of R. It will be observed that there are k superimposed square roots in (1). We leave it to the reader to prove that $R^{\frac{1}{2}}$ *is a field*, and that *the square root of every element of* $R^{\frac{1}{2}}$ *is also an element of* $R^{\frac{1}{2}}$. The importance of this field will appear subsequently.

The field $R^{\frac{1}{2}}$ may be the same as R. This happens, for example, when R is the field of complex numbers. On the other hand, $R^{\frac{1}{2}}$ need not be algebraic relative to R although the individual elements of $R^{\frac{1}{2}}$ are algebraic relative to R. This is the case when $R = R(1)$. For suppose that $R^{\frac{1}{2}}(1)$ is of degree n relative to R. Then the degree, relative to $R(1)$, of every element of $R^{\frac{1}{2}}$ is a divisor of n (p. 125). But $R^{\frac{1}{2}}(1)$ contains the positive real root of the equation

$$x^{2^m} - 2 = 0,$$

which is of degree 2^m relative to $R(1)$ (p. 68, Ex. 1). Since m may be chosen arbitrarily large, $R^{\frac{1}{2}}(1)$ is not algebraic relative to $R(1)$.

Excepting when $R^{\frac{1}{2}} = R$, $R^{\frac{1}{2}}$ contains one or more proper subfields—for example, the fields generated by those elements of $R^{\frac{1}{2}}$ which are not elements of R—which are algebraic relative to R. Concerning these subfields the following theorem is of great importance.

Theorem 1. *If $R' \neq R$ is a subfield of $R^{\frac{1}{2}}$ which is algebraic relative to R, then the degree of R' relative to R is a power of 2.*

The field R' contains a primitive element α which equals the sum of a finite number of terms of the form (1). With respect to this term let

$$a_k = h_k,\ a_{k-1} = h_{k-1} + g_k\sqrt{a_k},\ a_{k-2} = h_{k-2} + g_{k-1}\sqrt{a_{k-1}},\ \cdots .$$

It is obvious that (1) is contained in the field obtained by successive adjunctions to R of

$$\sqrt{a_k},\ \sqrt{a_{k-1}},\ \cdots,\ \sqrt{a_1}. \tag{2}$$

A similar set of square roots is formed for each term of α. These are now arranged in a single set

$$\sqrt{a_k},\ \sqrt{a_{k-1}},\ \cdots,\ \sqrt{a_1};\ \sqrt{b_l},\ \cdots,\ \sqrt{b_1};\ \cdots;\ \sqrt{u_p},\ \cdots,\ \sqrt{u_1}. \tag{3}$$

Now $\sqrt{a_k}$ is of degree 1 or 2 relative to R, and each of the other radicals of the set (3) is of degree 1 or 2 relative to the field generated by R and all the preceding radicals. Let us suppress all radicals in (3) of the first degree, forming the modified sequence of radicals

$$\sqrt{v_1},\ \sqrt{v_2},\ \cdots,\ \sqrt{v_q}, \tag{4}$$

each of which (except the first) is of degree 2 relative to the field

generated by R and all the preceding radicals, while $\sqrt{v_1}$ is of degree 2 relative to R. The field R'' generated by R and all the radicals (4) is clearly the same as the field generated by R and all the radicals (3). By Theorem 10, p. 132, the degree of R'' relative to R is 2^q. Since α is an element of R'' its degree relative to R is a divisor of 2^q and is therefore a power of 2.

Theorem 2. *All the conjugates, relative to R, of any element of $R^{\frac{1}{2}}$ are contained in $R^{\frac{1}{2}}$.*

Let α be an element of $R^{\frac{1}{2}}$. If α is in R, the theorem is evidently true. Suppose, then, that α is not in R, and form for α the sequence (4). Let $R_0 = R$, and let R_p be the field generated by R and the first p radicals of the set (4). We shall prove the theorem by mathematical induction: we shall assume that the theorem is true for every element of R_{p-1} and will prove that it is true for every element of R_p.

Since v_p is an element of R_{p-1}, its conjugates

$$v_p^{(1)},\ v_p^{(2)},\ \cdots,\ v_p^{(s)}$$

relative to R, are elements of $R^{\frac{1}{2}}$. If these conjugates satisfy the equation $F(v) = 0$, with coefficients in R, the roots of the equation $F(v^2) = 0$ are

$$\pm\sqrt{v_p^{(1)}},\ \pm\sqrt{v_p^{(2)}},\ \cdots,\ \pm\sqrt{v_p^{(s)}}.$$

The conjugates, relative to R, of $\sqrt{v_p}$ are included among these roots being the roots of that irreducible factor of $F(v^2)$ in R which has $\sqrt{v_p}$ as a root, and are therefore contained in $R^{\frac{1}{2}}$, since the square root of every element of $R^{\frac{1}{2}}$ is an element of $R^{\frac{1}{2}}$. The theorem is proved for $\sqrt{v_p}$.

Let

$$\beta = \sqrt{v_1} + b_2\sqrt{v_2} + \cdots + b_p\sqrt{v_p} \tag{5}$$

be a primitive element of R_p, the b's being elements of R (Theorem 9, p. 129). Since $\sqrt{v_k}$ is an element of $R_p = R(\beta)$,

$$\sqrt{v_k} = \varphi_k(\beta) \qquad (k = 1, \cdots, p),$$

where $\varphi_k(x)$ is a polynomial in R. (5) may now be written

$$\beta = \varphi_1(\beta) + b_2\varphi_2(\beta) + \cdots + b_p\varphi_p(\beta). \tag{6}$$

This equation remains valid when β is replaced by any conjugate β' of β relative to R. Hence

$$(7) \qquad \beta' = \varphi_1(\beta') + b_2\varphi_2(\beta') + \cdots + b_p\varphi_p(\beta').$$

But $\varphi_k(\beta')$ is a conjugate, relative to R, of $\sqrt{v_k} = \varphi_k(\beta)$ (Theorem 5, p. 124) and hence is an element of $R^{\frac{1}{2}}$. It follows from (7) that $R^{\frac{1}{2}}$ contains all the conjugates of β relative to R. Therefore $R^{\frac{1}{2}}$ contains all the conjugates, relative to R, of *any* element of R_p.

We have shown that if the theorem is true for every element of R_{p-1} it is also true for every element of R_p. Now the theorem is evidently true for every element of R_0; it is therefore true for every element of R_1. Being true for every element of R_1, it is true for every element of R_2; etc. We conclude that the theorem is true for every element of R_q and, in particular, for the selected element α.

THEOREM 3. *The conjugates, relative to R, of an element of $R^{\frac{1}{2}}$ generate with R a field whose degree, relative to R, is a power of* 2.

Let α be an element of $R^{\frac{1}{2}}$ and $\alpha_1, \cdots, \alpha_n$ its conjugates relative to R. These conjugates are contained in $R^{\frac{1}{2}}$ by Theorem 2. The field $R(\alpha_1, \cdots, \alpha_n)$ is therefore a subfield of $R^{\frac{1}{2}}$ and is clearly algebraic relative to R. The degree, relative to R, of $R(\alpha_1, \cdots, \alpha_n)$ is, by Theorem 1, a power of 2.

THEOREM 3′. *If α is an algebraic element relative to R, and if the conjugates of α relative to R generate with R a field whose degree, relative to R, is a power of 2, then α is contained in $R^{\frac{1}{2}}$.*

This is the converse of Theorem 3. The proof is difficult and will be omitted. The difficult part of the proof consists in showing that α is expressible in terms of radicals relative to R; it is then easy to show that these radicals must be square roots.

EXERCISES

1. Give examples of algebraic numbers which are not elements of $R^{\frac{1}{2}}(1)$.

2. Show that if $\cos\theta$ is an element of $R^{\frac{1}{2}}(1)$, so is $\cos\theta/2$.

3. Show that if the cartesian coordinates of two points are elements of R, the distance between the points is an element of $R^{\frac{1}{2}}$.

4. Show that the cartesian coordinates of the points of intersection of two circles are elements of $R^{\frac{1}{2}}$ if the coefficients of the equations of these circles are elements of R.

5. Show that if the coefficients of the cartesian equation of a circle are elements of R, the coordinates of its center are elements of R, while its radius is an element of $R^{\frac{1}{2}}$.

6. Show that if R is the field of real numbers, $R^{\frac{1}{2}}$ is the field of complex numbers.

7. Give examples of construction problems in whose solutions arbitrary elements are introduced.

68. Constructible elements. In order to apply algebraic methods to the analysis of construction problems it is convenient to introduce the notions of Analytic Geometry. A unit and a pair of rectangular axes will be assumed to have been chosen. Points are represented by their coordinates, lines and circles by their equations. The *algebraic* length of a line-segment may be a positive or a negative real number; its *geometric* length is the absolute value of its algebraic length.

We observe next that *the geometric figures of elementary geometry determine, and are determined by, one or more line-segments.* A point is determined by its coordinates, which are the algebraic distances from the point to the coordinate axes. An angle is determined by its trigonometric functions, which can be represented by line-segments. A line is determined by a pair of points which are, in turn, represented by line-segments; or by a point and the slope (when not infinite *) of the line, which are determined by line-segments; or by its equation, the ratios of whose coefficients (when none vanishes *) are representable as line-segments. A circle is determined by its center and radius, which are representable as line-segments; or by its equation, from which its center and radius can be determined.

We shall suppose, therefore, that certain line-segments are given, and that the solution of a proposed problem has been reduced to that of constructing one or more line-segments. We must now consider the problem: to determine all line-segments which can be constructed by ruler and compasses by means of a finite number of operations upon certain given line-segments.

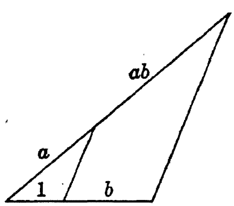

FIG. 12

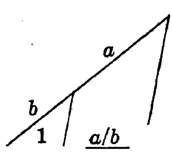

FIG. 13

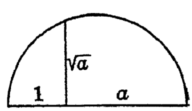

FIG. 14

It will be recalled that if line-segments of lengths a and b (real numbers or parameters) are given, it is possible to construct line-

* It is evident that the line is determined by a line-segment even in these

segments whose lengths are

$$a + b,\ a - b,\ ab,\ a/b\ (b \neq 0),\ \sqrt{a}\ (a > 0).$$

The figures on page 159 will refresh the student's memory as regards the last three constructions. It follows that if line-segments of lengths $a_1, a_2, \cdots, a_n$ are given, it is possible to construct a line-segment whose length is any real element which is expressible in terms of a finite number of radicals of index 2 (square roots) relative to the field $R(a_1, a_2, \cdots, a_n)$. With the notation of § 67, *every real element of* $R^{\frac{1}{2}}(a_1, a_2, \cdots, a_n)$ *is constructible;* that is, a line-segment whose length equals any real element of $R^{\frac{1}{2}}$ is constructible by ruler and compasses employing a finite number of operations.

Using these constructible line-segments it is possible to locate a point whose coordinates are real elements of $R^{\frac{1}{2}}$ or to draw a line or a circle the coefficients of whose equation are real elements of $R^{\frac{1}{2}}$. Let C denote the class of all line-segments, lines, points, and circles which are determined by the elements of $R^{\frac{1}{2}}$. The length of the line-segment joining two points (x_1, y_1) and (x_2, y_2) of C is $\sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2}$, which is an element of $R^{\frac{1}{2}}$; therefore no line-segment can be constructed whose length is not an element of $R^{\frac{1}{2}}$ by joining two points of the class C. The line determined by two points (x_1, y_1) and (x_2, y_2) of C belongs to C since the coefficients of its equation are elements of $R^{\frac{1}{2}}$. The point of intersection of two non-parallel lines of C belongs to C since its coordinates are found by solving two linear equations with coefficients in $R^{\frac{1}{2}}$. Finally the points of intersection of two circles of C or of a line and a circle of C belong to C. We conclude that *the class C is closed with respect to constructions by ruler and compasses;* that is, we cannot, by ruler and compasses alone, obtain any line-segment, point, line, or circle not in C from the line-segments, points, lines, and circles of the class C.

THEOREM 4. *A necessary and sufficient condition that a line-segment of length x be constructible by ruler and compasses from given line-segments of lengths $a_1, a_2, \cdots, a_n$ is that x be a real element of the field $R^{\frac{1}{2}}(a_1, a_2, \cdots, a_n)$.*

We have proved this theorem on the assumption that no new line-segments were introduced to facilitate the construction. Suppose now that new line-segments $b_1, b_2, \cdots, b_m$ are introduced. As stated in § 66, $b_1, b_2, \cdots, b_m$ must be entirely independent of

$a_1, a_2, \cdots, a_n$; that is, the b's must not be assumed to be functions of the a's. Since x, if constructible, must be an element of $R^{\frac{1}{2}}(a_1, \cdots, a_n; b_1, \cdots, b_m)$, and since x is independent of the b's, x must be an element of $R^{\frac{1}{2}}(a_1, a_2, \cdots, a_n)$ in any case.

We are now in a position to answer questions concerning the possibility of effecting constructions by ruler and compasses.

Example 1. To construct the edge of a cube whose volume is twice that of a cube whose edge is given.

Choosing the edge of the given cube as a unit, the volume of the required cube is 2. The edge of the required cube is therefore $\sqrt[3]{2}$. The problem is reduced to that of constructing a line-segment of length $\sqrt[3]{2}$. Now $\sqrt[3]{2}$ is not an element of $R^{\frac{1}{2}}(1)$; for the degree of $\sqrt[3]{2}$ relative to $R(1)$ is 3, whereas the degree of every element of $R^{\frac{1}{2}}(1)$ is a power of 2 by Theorem 1. The proposed construction is therefore impossible by ruler and compasses.

Example 2. To trisect a given angle.

Denoting the angle by θ (a parameter), a line can be constructed whose length is $t = \cos\theta$ with respect to a chosen unit. If it were possible to trisect the angle θ, it would be possible to construct a line of length $\cos\theta/3$. Since

$$4\cos^3\theta/3 - 3\cos\theta/3 = \cos\theta,$$

a line whose length is a root of the equation

$$4x^3 - 3x - t = 0$$

would be constructible. Since this equation is irreducible in $R(t)$ (Ex. 14, p. 64), its roots are of degree 3 relative to $R(t)$. The proposed construction is therefore impossible by ruler and compasses.

This result is not to be misinterpreted as meaning that *no angle can be trisected* (see Ex. 3 below). We have proved that an *arbitrary* angle cannot be trisected.

Example 3. To construct a square whose area equals the area of a given circle.

Taking the radius of the given circle as the unit, its area is π. The edge of the required square is $\sqrt{\pi}$. If the construction were possible $\sqrt{\pi}$, and hence π, would be an element of $R^{\frac{1}{2}}(1)$. Since the elements of $R^{\frac{1}{2}}(1)$ are algebraic numbers and π is not an algebraic number (p. 152), the proposed construction is impossible by ruler and compasses.

EXERCISES

Show that the following constructions can be effected by ruler and compasses whenever they are at all possible.

1. To construct a circle whose area is the sum of the areas of n given circles.

2. To inscribe a regular pentagon in a given circle. (See Ex. 15, p. 14.)

3. To trisect an angle whose cosine is $-\frac{11}{16}$.

4. To construct a triangle, given one side, the altitude to that side, and the opposite angle.

5. Through a given point to draw a line which cuts off a chord of given length from a given circle. [Find an equation satisfied by the slope of the line.]

6. To inscribe a square in a segment of a circle.

7. To draw two parallel chords of a given circle, given their sum and the distance between them.

8. To draw a circle through two given points such that a tangent line to this circle from a third given point has a given length.

9. To locate a point on a given line which is equidistant from a given point and a second given line.

10. To construct a right triangle given the sum of the sides including the right angle and the altitude on the hypotenuse.

Show that the following constructions cannot be effected by ruler and com-

11. To construct the radius of a sphere whose volume is the sum of the volumes of two spheres whose radii are given.

12. (a) To trisect an angle of 120°.

(b) To trisect an angle whose cosine is $\frac{2}{3}$.

13. To inscribe a regular polygon of 9 sides in a given circle.

14. To construct a line whose length equals the circumference of a given circle.

15. To locate a point on a given line the product of whose distances from three given points on the line is a given constant.

16. To inscribe an isosceles triangle of given area in a given circle.

17. To construct an isosceles triangle whose perimeter and area are given.

18. To locate on a given circle a point which is equidistant from a given point and a given line.

19. To draw a chord of a given circle which forms, with the tangent lines to the circle at its extremities, a triangle of given perimeter.

20. To construct a right triangle given the perimeter and the median to one of the legs.

69. Irreducibility of the polynomial whose roots are the primitive nth roots of unity. We proved in § 6 that if ϵ is a primitive nth root of unity and if $c_1, \cdots, c_h$ are the positive integers $\leq n$ and prime to n, then $\epsilon^{c_1}, \cdots, \epsilon^{c_h}$ are the primitive nth roots of unity. We have also seen that the coefficients of the primary polynomial

$$F_n(x) = (x - \epsilon^{c_1}) \cdots (x - \epsilon^{c_h}),$$

whose roots are the primitive nth roots of unity are integers (Ex. 25, p. 39). For the purposes of the next section we shall now prove that *the polynomial $F_n(x)$ is irreducible in $R(1)$*. The case in which n is a prime number was treated in § 27. A number of proofs of this important theorem are known, all of which involve the Theory of Numbers to a greater or lesser extent. The propositions of the Theory of Numbers which are required in our proof are developed in the lemmas.

LEMMA 1. *Let c, n, and $N \geq 1$ be integers of which c and n are relatively prime. Let P be the product of all the prime numbers $\leq N$ which are not divisors of cn; in the event that there are no such prime numbers, let $P = 1$. Every prime number which is a divisor of the integer $c' = c + nP$ is $> N$.*

Every prime number $p \leq N$ is a divisor of c or of nP but not of both these numbers since c and nP are relatively prime. If p is a divisor of c it cannot be a divisor of c' since in that case it would be a divisor of $nP = c' - c$. If p is a divisor of nP it cannot be a divisor of c' since in that case it would be a divisor of $c = c' - nP$. Therefore every prime number which is a divisor of c' is $> N$.

LEMMA 2. (FERMAT.) *If p is a prime number and a any integer, $a^p - a$ is divisible by p.*

With the aid of the expansion by the Binomial Theorem of $(a \pm 1)^p$ it is readily proved that

$$(a \pm 1)^p - (a \pm 1) = a^p - a + pb,$$

where b is an integer. Let the student complete the proof by mathematical induction.

LEMMA 3. *If $f(x)$ is a primary polynomial with integral coefficients and $g(x)$ is the primary polynomial whose roots are the pth powers of the roots of $f(x)$, where p is a prime number, then*

$$f(x) - g(x) = p\psi(x),$$

*where $\psi(x)$ is a polynomial with integral coefficients.**

* In special cases $f(x)$ and $g(x)$ may be identical and $\psi(x) = 0$.

Let $\alpha_1, \cdots, \alpha_m$ be the roots of $f(x)$. The kth elementary symmetric functions of the roots of $f(x)$ and of $g(x)$ are

$$\sigma_k = \Sigma\alpha_1\alpha_2 \cdot \quad \alpha_k$$

and

$$\sigma_k' = \Sigma\alpha_1^p\alpha_2^p \cdots \alpha_k^p$$

respectively. Hence

$$\sigma_k^p - \sigma_k' = pG,$$

where G is a symmetric function, with integral coefficients, of $\alpha_1, \cdots, \alpha_m$ and therefore equals an integer (Theorem 9, p. 108). Since, by Lemma 2,

$$\sigma_k^p = \sigma_k + pH,$$

where H is an integer,

$$\sigma_k - \sigma_k' = p(G - H).$$

We conclude that every coefficient of the polynomial $f(x) - g(x)$ is divisible by p.

THEOREM 5. *The primary polynomial whose roots are the primitive nth roots of unity is irreducible in the field of rational numbers.*

Let ϵ be a primitive nth root of unity, and let $f(x)$, of degree m, be the primary irreducible polynomial in $R(1)$ of which ϵ is a root. $f(x)$ is a divisor of the primary polynomial $F_n(x)$ whose roots are the primitive nth roots of unity. Therefore

$$f(x) = (x - \epsilon^{a_1}) \cdots (x - \epsilon^{a_m}),$$

where $a_1, \cdots, a_m$ are distinct positive integers $\leq n$ and prime to n. We shall prove that $f(x) = F_n(x)$.

Let p be a prime number, and let $g(x)$ be the primary polynomial whose roots are $\epsilon^{pa_1}, \cdots, \epsilon^{pa_m}$. If σ_k and σ_k' are the kth elementary symmetric functions of the roots of $f(x)$ and of $g(x)$ respectively,

$$f(x) = x^m - \sigma_1 x^{m-1} + \cdot \quad + (-1)^m\sigma_m,$$
$$g(x) = x^m - \sigma_1' x^{m-1} + \quad \cdot + (-1)^m\sigma_m'.$$

The coefficients of $f(x)$ and of $g(x)$ are integers (Theorem 4, p. 65; Theorem 9, p. 108). Now

$$\sigma_k = \Sigma\epsilon^{a_1} \qquad \epsilon^{a_k} \qquad \text{(symmetric function)},$$

the right member of which consists of

$$\binom{m}{k} = \frac{m(m-1)\cdots(m-k+1)}{k!}$$

terms each equal to 1 in absolute value. Hence

$$|\sigma_k| \leq \binom{m}{k} < 2^m * \leq 2^n$$

Similarly $|\sigma_k'| < 2^n$. By Lemma 3,

$$f(x) - g(x) = p(t_0x^m + t_1x^{m-1} + \cdots + t_m),$$

where $t_0, t_1, \cdots, t_m$ are integers. Consequently

$$|pt_k| = |\sigma_k - \sigma_k'| \leq |\sigma_k| + |\sigma_k'| < 2^n + 2^n = 2^{n+1}.$$

If $p > 2^{n+1}$, this inequality implies that $t_k = 0$. Therefore if $p > 2^{n+1}$, *then* $f(x) = g(x)$, *and the pth power of every root of* $f(x)$ *is also a root of* $f(x)$.

We now apply Lemma 1. Let c be any integer prime to n, let $N = 2^{n+1}$, and let $c' = c + nP$, where P has the value defined in Lemma 1. Write c' as the product of prime numbers:

$$c' = p_1p_2 \cdots p_r.$$

By Lemma 1 each of these primes is $> 2^{n+1}$. Therefore, since ϵ is a root of $f(x)$, so is ϵ^{p_1}. Since ϵ^{p_1} is a root of $f(x)$, so is $(\epsilon^{p_1})^{p_2} = \epsilon^{p_1p_2}$. Continuing thus we infer that $\epsilon^{c'}$ is a root of $f(x)$. But $\epsilon^{c'} = \epsilon^c\epsilon^{nP} = \epsilon^c$ since $\epsilon^n = 1$. Therefore if c is any integer prime to n, ϵ^c is a root of $f(x)$. We conclude that every primitive nth root of unity is a root of $f(x)$ so that $f(x) = F_n(x)$.

70. Inscribable regular polygons. In this section we shall discuss the question: For what values of the integer $n \geq 3$ is it possible to inscribe, by ruler and compasses, a regular polygon of n sides in a given circle?

The given circle will be taken as the unit circle in the plane of complex numbers and the point 1 will be chosen as one vertex of the regular polygon. A regular polygon of n sides can be inscribed in the unit circle, with one vertex at the point 1, if and only if (see Figure 15) the lines

$$ON = \cos 2\pi/n, \qquad NP_1 = \sin 2\pi/n$$

* Because $\binom{m}{k}$ is a term of the expansion of $(1+1)^m$

are constructible. Therefore $\cos 2\pi/n$, $\sin 2\pi/n$, and

$$\epsilon = \cos 2\pi/n + i \sin 2\pi/n$$

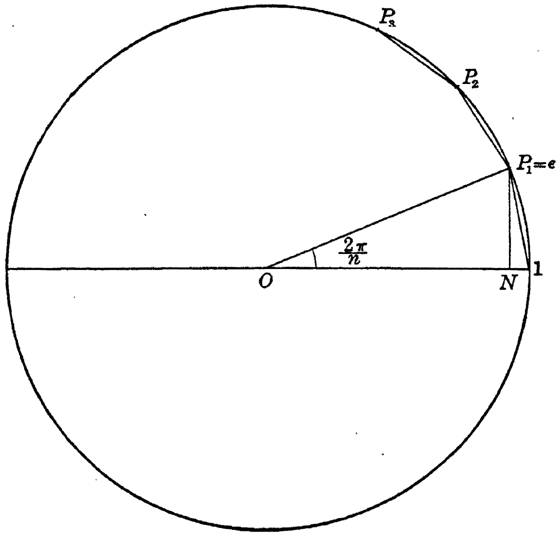

FIG. 15

must be elements of $R^{\frac{1}{2}}(1)$. *A regular polygon of n sides is inscribable in a circle by ruler and compasses if, and only if, the nth roots of unity are elements of* $R^{\frac{1}{2}}(1)$.

Since the degree, relative to $R(1)$, of every element of $R^{\frac{1}{2}}(1)$ is a power of 2 (Theorem 1), only those roots of unity are contained in $R^{\frac{1}{2}}(1)$ which satisfy irreducible equations in $R(1)$ whose degrees are powers of 2. Now the primitive nth roots of unity satisfy an equation in $R(1)$ of degree $\varphi(n)$, where $\varphi(n)$ is the number of positive integers $< n$ and prime to n, and this equation is irreducible in $R(1)$ (Theorem 5). It follows that the primitive nth roots of unity, and hence all the nth roots of unity, are elements of $R^{\frac{1}{2}}(1)$ if, and only if, $\varphi(n)$ is a power of 2. *A regular polygon of n sides is inscribable in a circle by ruler and compasses if, and only if,* $\varphi(n)$ *is a power of* 2.

The number-theoretic function $\varphi(n)$ is called *Euler's φ-function* and plays an important rôle in the elementary Theory of Numbers,

where it is shown that if

$$n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r},$$

the p's being distinct prime numbers and the a's positive integers, then

$$\varphi(n) = p_1^{a_1-1} p_2^{a_2-1} \cdots p_r^{a_r-1}(p_1 - 1)(p_2 - 1) \cdots (p_r - 1).$$

From this formula it follows that $\varphi(n)$ is a power of 2 if, and only if, n is not divisible by the square of a prime number > 2 and each odd prime factor of n has the form $1 + 2^s$.

THEOREM 6. *A regular polygon of $n \geq 3$ sides is inscribable in a circle by ruler and compasses if, and only if, n is a power of 2 or*

$$n = 2^a p_1 p_2 \cdots p_r, \qquad (a \geq 0,\ r \geq 1),$$

where the p's denote distinct prime numbers of the form $1 + 2^s$.

EXERCISES

1. Show that regular polygons of 3, 4, 5, 6, 8, 10, 12, 15, 16, 17, 20, 24, 34, and 257 sides are inscribable.

2. Show that regular polygons of 7, 9, 11, 13, 18, 25, 35, 100, and 105 sides are not inscribable.

3. Show that $1 + 2^s$ is not a prime number if s is not a power of 2.

71. Construction of a regular polygon of 17 sides. Since $\varphi(17) = 2^4$, a regular polygon of 17 sides can be inscribed in a circle by ruler and compasses. To determine the details of the construction of a regular polygon of 17 sides we shall solve by radicals the equation

$$z^{16} + z^{15} + \qquad + z + 1 = 0,$$

whose roots are the primitive 17th roots of unity. We shall find that the radicals which occur are square roots. By examining these square roots and the equations which yield them we are led to a construction by ruler and compasses of a regular polygon of 17 sides.

Following Gauss, the roots are arranged in the order *

$$(1) \qquad \epsilon,\ \epsilon^3,\ \epsilon^9,\ \epsilon^{10},\ \epsilon^{13},\ \epsilon^5,\ \epsilon^{15},\ \epsilon^{11},\ \epsilon^{16},\ \epsilon^{14},\ \epsilon^8,\ \epsilon^7,\ \epsilon^4,\ \epsilon^{12},\ \epsilon^2,\ \epsilon^6,$$

each of which is the *cube* of the preceding, the first being the cube

* See Ex. 1 and 2 below.

of the last. Here

(2) $$\epsilon = \cos\theta + i\sin\theta, \qquad (\theta = 2\pi/17).$$

The sums of the alternate terms of (1) are now formed:

(3) $$\begin{aligned} y_1 &= \epsilon + \epsilon^9 + \epsilon^{13} + \epsilon^{15} + \epsilon^{16} + \epsilon^8 + \epsilon^4 + \epsilon^2, \\ y_2 &= \epsilon^3 + \epsilon^{10} + \epsilon^5 + \epsilon^{11} + \epsilon^{14} + \epsilon^7 + \epsilon^{12} + \epsilon^6. \end{aligned}$$

Since the sum of *all* the 17th roots of unity is 0,

$$\epsilon + \epsilon^2 + \cdots + \epsilon^{16} = -1.$$

With the aid of this relation it is readily verified that

$$y_1 + y_2 = -1, \qquad y_1 y_2 = 4.$$

Therefore y_1 and y_2 satisfy the equation

(4) $$y^2 + y - 4 = 0,$$

whose roots are $(-1 \pm \sqrt{17})/2$. To determine which of these is y_1 and which y_2, we observe that, by (3)

$$\begin{aligned} y_1 &= (\epsilon + \epsilon^{16}) + (\epsilon^2 + \epsilon^{15}) + (\epsilon^4 + \epsilon^{13}) + (\epsilon^8 + \epsilon^9) \\ &= 2\cos\theta + 2\cos 2\theta + 2\cos 4\theta + 2\cos 8\theta, \end{aligned}$$

which is *positive*. Therefore

(5) $$y_1 = \frac{-1 + \sqrt{17}}{2}, \qquad y_2 = \frac{-1 - \sqrt{17}}{2}.$$

Four sums are now formed from the alternate terms of (3):

(6) $$\begin{aligned} x_1 &= \epsilon + \epsilon^{13} + \epsilon^{16} + \epsilon^4 = 2\cos\theta + 2\cos 4\theta, \\ x_2 &= \epsilon^9 + \epsilon^{15} + \epsilon^8 + \epsilon^2 = 2\cos 2\theta + 2\cos 8\theta, \\ x_3 &= \epsilon^3 + \epsilon^5 + \epsilon^{14} + \epsilon^{12} = 2\cos 3\theta + 2\cos 5\theta, \\ x_4 &= \epsilon^{10} + \epsilon^{11} + \epsilon^7 + \epsilon^6 = 2\cos 6\theta + 2\cos 7\theta. \end{aligned}$$

We find that x_1 and x_2 satisfy the equation

(7) $$x^2 - y_1 x - 1 = 0,$$

whose roots are $(-1 + \sqrt{17})/4 \pm (\sqrt{34 - 2\sqrt{17}})/4$. Since x_1 is positive while x_2 is negative (see last members of (6)), we have

$$
(8) \qquad
\begin{aligned}
x_1 &= \frac{-1+\sqrt{17}}{4} + \frac{\sqrt{34-2\sqrt{17}}}{4},\\
x_2 &= \frac{-1+\sqrt{17}}{4} - \frac{\sqrt{34-2\sqrt{17}}}{4}.
\end{aligned}
$$

Similarly x_3 and x_4 satisfy the equation

$$x^2 - y_2 x - 1 = 0,$$

from which it follows that

$$
(9) \qquad
\begin{aligned}
x_3 &= \frac{-1-\sqrt{17}}{4} + \frac{\sqrt{34+2\sqrt{17}}}{4},\\
x_4 &= \frac{-1-\sqrt{17}}{4} - \frac{\sqrt{34+2\sqrt{17}}}{4}.
\end{aligned}
$$

Again, forming the sums of the alternate terms of x_1 in (**6**), let

$$
(10) \qquad
\begin{aligned}
w_1 &= \epsilon + \epsilon^{16} = 2\cos\theta,\\
w_2 &= \epsilon^{13} + \epsilon^{4} = 2\cos 4\theta,
\end{aligned}
$$

which satisfy the equation

$$w^2 - x_1 w + x_3 = 0,$$

whose roots are

$$
(11) \qquad w_1 = \frac{x_1 + \sqrt{x_1^2 - 4x_3}}{2}, \qquad w_2 = \frac{x_1 - \sqrt{x_1^2 - 4x_3}}{2}.
$$

One more step is necessary to find ϵ. This step will be omitted as we have gone sufficiently far for our purpose. For (**11**) gives us the value of $w_1 = 2\cos\theta$, from which the angle $\theta = 2\pi/17$ can be constructed and the regular polygon of 17 sides completed. Equations (**5**), (**8**), (**9**), and (**11**) indicate the square roots which must be extracted for the purpose of constructing a regular polygon of 17 sides. It is not difficult to describe the construction with the aid of these results. We shall, however, give a more ingenious construction * based on (**3**), (**6**), and (**10**).

Construction

Let O be the center of the circle and AOA' a diameter. On the

* Due to H. W. Richmond, "To Construct a Regular Polygon of Seventeen Sides," *Mathematische Annalen*, Vol. 67 (1909), p. 459.

diameter $CC' \perp AA'$ lay off $OD = OA/4$. Join A and D. Locate E on OA so that $\alpha = \angle ODE = \frac{1}{4} \angle ODA$. Locate F on OA so that $\angle EDF = 45°$.

Let the perpendicular to OA at E intersect the circle drawn on OA as diameter in Q. With O as center and OQ as radius swing an arc intersecting the circle constructed on OF as diameter in R With F as center and FR as radius draw a circle intersecting OA in N_1 and N_4.

At N_1 erect a perpendicular to OA intersecting the given circle in P_1. Then AP_1 is a side of the regular polygon of 17 sides, and the polygon is readily completed. Incidentally, a perpendicular to OA at N_4 intersects the circle in a point P_4 which is the fourth vertex of the polygon if P_1 is regarded as the first.

Proof

From the construction, we have

$$\begin{aligned} (12) \qquad ON_1 \cdot ON_4 &= (OF + FR)(OF - FR) = OF^2 - FR^2 \\ &= OR^2 = OQ^2 = OA \cdot OE, \end{aligned}$$

$$(13) \qquad ON_1 + ON_4 = (OF + FR) + (OF - FR) = 2 \cdot OF,$$

$$(14) \qquad \tan 4\alpha = 4.$$

By means of the last equation (4) may be written

$$y^2 + 4y \cot 4\alpha - 4 = 0,$$

whose roots y_1 and y_2 are

$$-2 \cot 4\alpha \pm 2 \csc 4\alpha,$$

which are readily reduced to $-2 \cot 2\alpha$ and $2 \tan 2\alpha$. Since y_1 is positive and y_2 negative,

$$(15) \qquad y_1 = 2 \tan 2\alpha, \qquad y_2 = -2 \cot 2\alpha.$$

Therefore (7) may be written

$$x^2 - 2x \tan 2\alpha - 1 = 0,$$

whose roots x_1 and x_2 are

$$\tan 2\alpha \pm \sec 2\alpha = \frac{\sin 2\alpha \pm 1}{\cos 2\alpha}$$

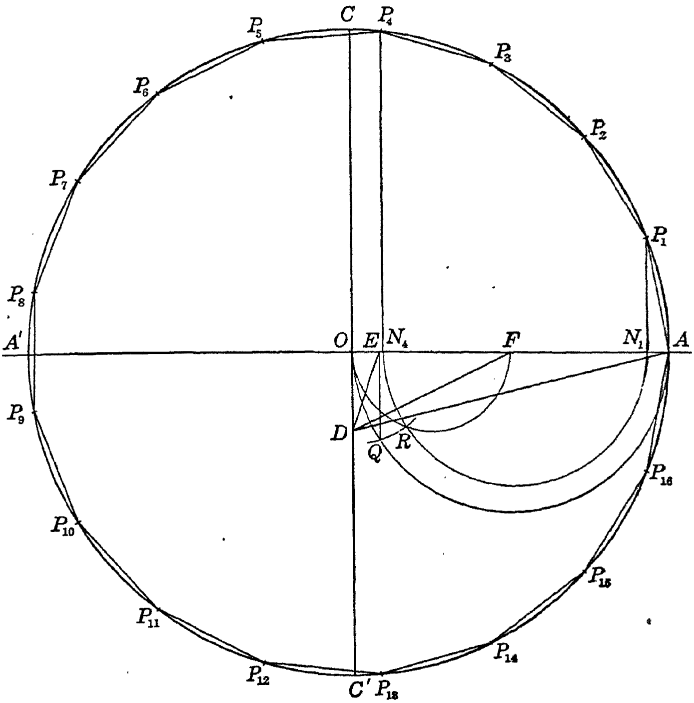

FIG. 16

Since x_1 is positive,

$$x_1 = \frac{1 + \sin 2\alpha}{\cos 2\alpha} = \frac{1 - \cos(2\alpha + 90°)}{\sin(2\alpha + 90°)}$$

$$\frac{2\sin^2(\alpha + 45°)}{2\sin(\alpha + 45°)\cos(\alpha + 45°)} = \tan(\alpha + 45°).$$

Similarly

$$x_2 = \frac{\sin 2\alpha - 1}{\cos 2\alpha} = -\cot(\alpha + 45°) = \tan(\alpha + 135°).$$

Similar expressions may be obtained for x_3 and x_4. We then have

$$x_1 = 2(\cos\theta + \cos 4\theta) = \tan(\alpha + 45°),$$

$$(16)\qquad \begin{aligned} x_2 &= 2(\cos 2\theta + \cos 8\theta) = \tan(\alpha + 135°),\\ x_3 &= 2(\cos 3\theta + \cos 5\theta) = \tan\alpha,\\ x_4 &= 2(\cos 6\theta + \cos 7\theta) = \tan(\alpha + 90°). \end{aligned}$$

Taking the radius $OA = 1$, and employing the trigonometric identity

$$\cos 3\theta + \cos 5\theta = 2\cos\theta\cos 4\theta,$$

we have by (**16**),

$$(17)\qquad \begin{aligned} 2\cos\theta + 2\cos 4\theta &= \tan(\alpha + 45°) = 4\,OF,\\ 2\cos\theta\cdot 2\cos 4\theta &= \tan\alpha = 4\,OE. \end{aligned}$$

Therefore, by (**12**) and (**13**),

$$(18)\qquad \begin{aligned} ON_1 + ON_4 &= \cos\theta + \cos 4\theta,\\ ON_1\cdot ON_4 &= \cos\theta\cos 4\theta. \end{aligned}$$

It follows that ON_1 and ON_4 satisfy the same quadratic equation as $\cos\theta$ and $\cos 4\theta$. Since $ON_1 > ON_4$ and $\cos\theta > \cos 4\theta$, we conclude that

$$(19)\qquad ON_1 = \cos\theta, \qquad ON_4 = \cos 4\theta.$$

EXERCISES

1. Show that the primitive 17th roots of unity can be arranged in order so that each root is the *fifth* power of the preceding, the first being the fifth power of the last. Show that the sums of the alternate terms of this arrangement are the same as those of the text.

2. Show that the primitive 17th roots of unity cannot be arranged in order so that each root is the *square* of the preceding.

3. Express the fifth roots of unity in terms of radicals by Gauss's method.

4. Show that

(a) $2\cos 3\theta + 2\cos 5\theta = \tan\alpha$,
$2\cos 3\theta\cdot 2\cos 5\theta = \tan(\alpha + 135°)$

(b) $2\cos 2\theta + 2\cos 8\theta = \tan(\alpha + 135°)$,
$2\cos 2\theta\cdot 2\cos 8\theta = \tan(\alpha + 90°)$

(c) $2\cos 6\theta + 2\cos 7\theta = \tan(\alpha + 90°)$,
$2\cos 6\theta\cdot 2\cos 7\theta = \tan(\alpha + 45°)$.

These results are similar to (**17**) and lead to independent constructions of the third and fifth, second and eighth, and sixth and seventh vertices respectively of the regular polygon of 17 sides.

MISCELLANEOUS EXERCISES

1. Show that if $z + z^{-1} = 2\cos\theta$, then $z^n + z^{-n} = 2\cos n\theta$.

2. Show that the line joining the points z_1 and z_2 is parallel to the line joining the points z_3 and z_4 if, and only if, $\dfrac{z_1 - z_2}{z_3 - z_4}$ is a real number.

3. Show that $|z_1 + z_2|^2 + |z_1 - z_2|^2 = 2(|z_1|^2 + |z_2|^2)$.

4. Show that if $|z_1| = t|z_2|$, where t is real and ≥ 0, then $|t^2 z_2 - z_1| = t|z_2 - z_1|$.

5. Show that if a and b are distinct complex numbers, the locus of a point z which satisfies the equation

$$|z - a| = k|z - b|, \qquad (k > 0, k \neq 1)$$

is a circle whose center is the point $\dfrac{k^2 b - a}{k^2 - 1}$ and whose radius is $\dfrac{|a - b|}{k^2 - 1}$.

6. Find the remainder of the division of $x^{60} - 1$ by $x^3 - a$.

Ans. $a^{20} - 1$.

7. Find the remainder of the division of $x^{100} - 1$ by $x^3 - a$.

Ans. $a^{33}x - 1$.

8. Show that if $f(x)$ is a polynomial,

$$(x - y)f(z) + (y - z)f(x) + (z - x)f(y)$$

is divisible by $(x - y)(y - z)(z - x)$.

9. Show that the remainder of the division of the polynomial $f(x)$ by $(x - a)(x - b)$, $(a \neq b)$ is

$$\frac{f(a) - f(b)}{a - b}x + \frac{af(b) - bf(a)}{a - b}$$

10. Show that if a, d, and n are positive integers and d is a divisor of n, then $x^{a^d - 1} - 1$ is a divisor of $x^{a^n - 1} - 1$.

11. Show that if n and m are positive integers,

$$(x^n - 1)(x^{n+1} - 1) \cdots (x^{n+m-1} - 1)$$

is divisible by

$$(x - 1)(x^2 - 1) \cdots (x^m - 1).$$

12. Show that if p is a prime number > 2, then

$$(x - 1)(x^2 - 1) \cdots (x^{p-1} - 1) - p$$

is divisible by $\dfrac{x^p - 1}{x - 1}$.

13. Show that if p is a prime number > 2, then

$$(x - t)(x^2 - t) \cdots (x^{p-1} - t) - \frac{t^p - 1}{t - 1}$$

is divisible by $\dfrac{x^p - 1}{x - 1}$.

14. Show that if

$$P(x) = (x + 1)^{2n} + 2x(x + 1)^{2n-1} + \cdots 2^n x^n (x + 1)^n,$$

then $(x - 1)P(x) + (x + 1)^{2n+1}$ is divisible by x^{n+1}. (*Nouvelles Annales de Math.* (1919), p. 438.)

15. Let $A(x)$ and $B(x)$ be two polynomials of degrees n and m respectively in a field R. Prove that unique polynomials $C_0, C_1, \cdots, C_k$ in R, each of degree $< m$, exist such that

$$A = C_0 + C_1 B + C_2 B^2 + \cdots + C_k B^k,$$

where k is the largest integer $\leq n/m$.

16. Show that if r is prime to n, then $F_n(x^r)$ is divisible by $F_n(x)$, where $F_n(x)$ is the primary polynomial whose roots are the primitive nth roots of unity.

17. Show that if $f(x^r)$, $(r \geq 2)$, is divisible by the polynomial $f(x)$, then every root of $f(x)$ is 0 or a root of unity.

18. Show that if ϵ is a primitive nth root of unity and $f(x)$ is a polynomial of degree $\leq n - 1$, then

$$f(x) + f(\epsilon x) + \cdots + f(\epsilon^{n-1}x) = nf(0).$$

19. Show that if p is a prime > 2, and ϵ is a primitive pth root of unity, then

$$(x - 1)^p + (x - \epsilon)^p + \cdots + (x - \epsilon^{p-1})^p = p(x^p - 1).$$

20. Let ϵ be an nth root of unity different from 1, and let

$$f(x) = x^{n-1} + x^{n-2} + \cdots + x + 1.$$

Show that

$$f'(\epsilon) = \frac{n}{\epsilon(\epsilon - 1)}.$$

21. With the same notation, show that

$$\epsilon + 2\epsilon^2 + \qquad + (n - 1)\epsilon^{n-1} \qquad \overline{\epsilon - 1}$$

22. Let α be a primitive nth root of unity and β a primitive mth root of unity. Show that if n and m are relatively prime then $\alpha\beta$ is a primitive nmth root of unity.

23. Solve the equation $(z + i)^n + (z - i)^n = 0$.

Ans. $z = \cot (2k + 1)\pi/2n$, $(k = 0, 1, \cdots, n - 1)$.

24. Solve the equation $(z + i)^n - (z - i)^n = 0$.

Ans. $z = \cot k\pi/n$, $(k = 1, \cdots, n - 1)$.

25. Show that if a is a real number all the roots of the equation $(z + a)^n + (z - a)^n = 0$ lie on the axis of pure imaginaries.

26. Show that the roots of the equation $(z^m - 1)^n = 1$ are

$$\sqrt[m]{2\cos\frac{k\pi}{n}}\left[\cos\left(\frac{k\pi}{nm} + \frac{2l\pi}{m}\right) + i\sin\left(\frac{k\pi}{nm} + \frac{2l\pi}{m}\right)\right],$$

$$\begin{pmatrix} k = 0, 1, \cdots, n - 1 \\ l = 0, 1, \cdots, m - 1 \end{pmatrix}$$

27. Show that

$$\prod_{k=0}^{n-1} \sin(\varphi + k\pi/n) = \frac{\sin n\varphi}{2^{n-1}}.$$

[Substitute $z = \cos 2\varphi + i \sin 2\varphi$ in the identity

$$1 - z^n = \prod_{k=0}^{n-1} (1 - \epsilon^k z),$$

and apply trigonometric formulas.]

28. Deduce that $\sum_{k=0}^{n-1} \cot(\varphi + k\pi/n) = n \cot n\varphi$, where $\varphi \neq m\pi/n$, m being an integer.

29. Show that the only primary polynomials of degree 2 with integral coefficients whose roots are roots of unity are

$$x^2 \pm 1, \qquad x^2 \pm x + 1, \qquad x^2 \pm 2x + 1.$$

30. Prove that if the absolute value of every root of a primary polynomial with integral coefficients is 1, these roots must be roots of unity. [Consider the equation whose roots are the mth powers of the roots of the given equation, $m = 1, 2, \cdots$. Only a finite number of these equations are distinct.]

31. Show that if $F_n(x)$ is the primary polynomial whose roots are the primitive nth roots of unity, then

$$F_n(1) = \begin{cases} 0 \text{ if } n = 1, \\ p \text{ if } n \text{ is a power of the prime } p, \\ 1 \text{ otherwise.} \end{cases}$$

[Prove by mathematical induction, using the result of Ex. 24, p. 39.]

32. Show that the length of a side of a regular polygon of 11 sides, inscribed in a circle of radius 1, is a root of the equation

$$x^5 - \sqrt{11}(x^4 - 3x^2 - 1) - 11x = 0.$$

(*American Mathematical Monthly* (1922), p. 91.)

33. Show that the remainder obtained when the polynomial $f(x)$ is

divided by the polynomial $F(x) = (x - x_1) \cdot (x - x_n)$, where $x_1, \cdots, x_n$ are distinct is

$$\sum_{i=1} \frac{f(x_i)F(x)}{(x - x_i)F'(x_i)}.$$

34. Let r be a root of a polynomial $f(x)$ with distinct roots, and let $P(x) = \dfrac{f(x)}{f'(r)(x - r)}$. Show that the remainder of the division of $[P(x)]^2$ by $f(x)$ is $P(x)$.

35. Let $A(x) = a(x - \alpha_1) \cdots (x - \alpha_n)$ and

$$B(x) = b(x - \beta_1) \cdots (x - \beta_m),$$

$(ab \neq 0)$ be two relatively prime polynomials, each having distinct roots. Define

$$F(x) = \sum_{i=1}^{n} \frac{A(x)}{(x - \alpha_i)A'(\alpha_i)B(\alpha_i)},$$

$$G(x) = \sum_{i=1}^{m} \frac{B(x)}{(x - \beta_i)B'(\beta_i)A(\beta_i)}.$$

Prove that $A(x)G(x) + B(x)F(x) = 1$.

36. Let $f_1(x), \cdots, f_k(x)$ be non-constant polynomials in a field R, each prime to every other. Let $f(x)$ be their product and

$$g_i(x) = f(x)/f_i(x), \qquad (i = 1, \cdots, k).$$

Prove that unique polynomials $F_1(x), \cdots, F_k(x)$ in R exist whose degrees are less than those of $f_1(x), \cdots, f_k(x)$ respectively such that

$$g_1(x)F_1(x) + \cdots + g_k(x)F_k(x) = 1.$$

37. Show that if $F(x) = (x - x_1) \cdots (x - x_n)$, where $x_1, \quad x_n$ are distinct, then

$$\sum_{\substack{j=1 \\ j\neq i}}^{n} \frac{1}{x_i - x_j} = \frac{F''(x_i)}{2F'(x_i)}.$$

38. Show that the unique polynomial $f(x)$ of degree $\leq 2n - 1$ which satisfies the conditions

$$f(x_i) = y_i,\ f'(x_i) = y_i', \qquad (i = 1, \cdots, n),$$

where the x's, the y's and the y''s are given and the x''s are distinct, is

$$f(x) = A(x) + F(x) \sum_{i=1}^{n} \frac{[y_i' - A'(x_i)]F(x)}{[F'(x_i)]^2(x - x_i)},$$

where $F(x) = (x - x_1) \cdots (x - x_n)$ and

$$A(x) = \sum_{i=1}^{n} \frac{y_i F(x)}{(x - x_i)F'(x_i)}.$$

39. Construct a polynomial $f(x)$ of lowest possible degree such that the curve $y = f(x)$ passes through the points (0, 5) and (1, 3) and has the slopes -3 and 1 respectively at these points.

40. Construct a polynomial $f(x)$ of lowest possible degree such that the curve $y = f(x)$ passes through the points $(-1, 12)$, $(0, 4)$, and $(1, 8)$ and has a horizontal tangent line at each of these points.

41. Construct a polynomial of lowest possible degree which yields the remainders $-5x^2 + 2x - 8$ and $23x + 16$ when divided by $x^3 - x$ and $x^2 - 4$ respectively.

42. Construct a primary polynomial of lowest possible degree which yields the remainders $9x - 7$ and $9x - 6$ when divided by $x^2 + x - 3$ and $x^2 + 2x - 1$ respectively. *Ans.* $x^4 + 2x^3 - 3x^2 + 5x - 4$.

43. Let σ_k be the kth elementary symmetric function of n positive numbers. Prove that

(a) $\sigma_k \leq \sigma_1 \sigma_{k-1}/k$, (b) $\sigma_k \leq \sigma_1{}^k/k!$.

44. Show that if $f(x) = f(1 - x)$, where $f(x)$ is a polynomial, there exists a polynomial $F(x)$ such that $f(x) = F(x - x^2)$; and conversely.

45. Show that

$$\frac{\quad}{x(x+1)(x+2)} \qquad \frac{\quad}{(x+n)} \qquad \frac{1}{x} \cdots \frac{\binom{n}{1}}{x+1} + \frac{\binom{n}{2}}{x+2} \cdots \qquad + \frac{(-1)^n}{x+n}.$$

46. Prove that a non-constant polynomial $f(x)$ in a field R is not a periodic function; that is, there exists no element $h \neq 0$ of R such that $f(x + h) = f(x)$.

47. Prove that a polynomial which is irreducible in a field R cannot have two distinct roots whose difference is an element of R.

48. Show that if $F(x) = (x - x_1) \cdots (x - x_n)$ is a polynomial of degree $n \geq 2$ with distinct roots, then

$$\frac{\quad}{F'(x_1)} + \qquad \frac{\quad}{F'(x_n)} \quad 0.$$

[Use Ex. 4 (b), p. 58.]

49. Show that if $f(x)$ is a polynomial of degree n in a field R, every polynomial in R of degree $\leq n$ may be written uniquely in the form

$$c_0 f(x) + c_1 f'(x) + \qquad + c_n f^{(n)}(x),$$

where the c's are elements of R.

50. Let $A(x)$ and $B(x)$ be polynomials of degree n. Show that

$$A(x)B^{(n)}(x) - A'(x)B^{(n-1)}(x) + A''(x)B^{(n-2)}(x) - \cdots (-1)^n A^{(n)}(x)B(x)$$

is a constant. [Show that its derivative is 0.]

51. Construct the equation whose roots are

$$2(\cos 3\theta - \cos\theta), \qquad 2(\cos\theta - \cos 2\theta), \qquad 2(\cos 2\theta - \cos 3\theta),$$

where $\theta = 2\pi/7$. *Ans.* $x^3 - 7x + 7 = 0$.

52. Show that if $R(\sqrt{a})$ and $R(\sqrt{b})$ are quadratic fields relative to R, then

$$R(\sqrt{a}, \sqrt{b}) = R(\sqrt{a} + \sqrt{b}) = R(\sqrt{a} - \sqrt{b}), \qquad (a \neq b).$$

53. Show that if a polynomial $f(x)$ is irreducible in R but is reducible in each of the distinct relative quadratic fields $R(\sqrt{a})$ and $R(\sqrt{b})$, then

$$f(x) = cP(x, \sqrt{a} + \sqrt{b})P(x, \sqrt{a} - \sqrt{b})P(x, -\sqrt{a} + \sqrt{b})P(x, -\sqrt{a} - \sqrt{b}),$$

where c is an element of R and $P(x, y)$ is a polynomial with coefficients in R. [Use Theorem 8, p. 129.]

54. Show that a polynomial in a field R which is reducible in each of the distinct relative quadratic fields $R(\sqrt{a})$ and $R(\sqrt{b})$ is also reducible in $R(\sqrt{ab})$.

55. Solve the equation $x^3 - 3x + \dfrac{-3+i}{2} = 0$ by the Cardan formulas and reduce the roots to the form

$$x_1 = 2^{-\frac{1}{6}}(\cos 15^\circ + i\sin 15^\circ) + 2^{\frac{1}{6}}(\cos 15^\circ - i\sin 15^\circ),$$
$$x_2 = -2^{-\frac{1}{6}}(\cos 45^\circ - i\sin 45^\circ) - 2^{\frac{1}{6}}(\cos 45^\circ + i\sin 45^\circ),$$
$$x_3 = -2^{-\frac{1}{6}}(\cos 75^\circ + i\sin 75^\circ) - 2^{\frac{1}{6}}(\cos 75^\circ - i\sin 75^\circ).$$

56. Show that $\dfrac{a}{4}(9 \pm \sqrt{33})$ are double roots of the equation

$$(x - 2a)(2x + a)(x + 6a)(2x - 3a) - 4ax(3x - 4a)(4x - 9a) = 0.$$

(*Nouvelles Annales de Math.* (1917), p. 38.)

57. Show that the equation

$$128(x - a)^6 + 432a(x - b)(x - a)^4 - 729a^3(x - b)^3 = 0$$

has two double roots. (*Nouvelles Annales de Math.* (1906), p. 275.)

58. Show that if α is a root of the equation

$$x^3 - 3tx^2 + 3(t - 1)x + 1 = 0,$$

then $1/(1 - \alpha)$ and $1 - 1/\alpha$ are also roots.

59. Show that the sum of the square roots of the roots of the quadratic equation $a_0x^2 + a_1x + a_2 = 0$ satisfies the equation

$$(a_0y^2 + a_1)^2 - 4a_0a_2 = 0.$$

What are the other roots of this equation?

60. Show that

$$\sqrt[3]{1 + \tfrac{2}{3}\sqrt{\tfrac{7}{3}}} + \sqrt[3]{1 - \tfrac{2}{3}\sqrt{\tfrac{7}{3}}} \quad 1.$$

The indicated cube roots are understood to be real. (*Mathesis*, (1907), p. 277.)

61. Solve the simultaneous equations

$$x^3 + y^3 = -4a^3,$$

$$\frac{1}{x} + \frac{1}{y} \quad \frac{1}{a}$$

(*Mathesis* (1908), p. 229.)

62. Find the lengths of the edges of two cubes if the sum of the areas of their faces is 38 sq. ft. and the sum of their volumes is 15 cu. ft.

Ans. $\sqrt{33}$ ft.

63. Find the sum of the products of the integers $1, 2, \cdots, n$ taken two at a time. *Ans.* $\frac{1}{24}n(n-1)(n+1)(3n+2)$.

64. Find the sum of the products of the integers $1, 3, \cdots, 2n-1$ taken two at a time.

65. Show that if $A(x)$ and $B(x)$ are relatively prime polynomials of degree ≥ 1, with integral coefficients, there exists only a finite number of integers k (possibly none) such that the integer $A(k)$ is divisible by the integer $B(k)$.

66. Let $A(x)$ and $B(x)$ be polynomials with integral coefficients. Show that if $A(k)/B(k)$ is an integer for every integer k, then the polynomial $A(x)$ is divisible by the polynomial $B(x)$.

67. Show that if $A(x)$ and $B(x)$ are relatively prime polynomials of degree ≥ 1, with integral coefficients, the g.c.d. of the integers

$$A(k) \text{ and } B(k), \qquad (k = 0, \pm 1, \pm 2, \cdots)$$

can assume only a finite number of distinct values.

68. A rectangular box has a volume of 14 cu. in. If each edge were increased by 1 in., the volume of the box would be 42 cu. in. If each edge were decreased by 1 in., the volume would be 2 cu. in. Find the dimensions of the box. *Ans.* $2, 3 \pm \sqrt{2}$ in.

69. Determine all integers t such that the equation

$$x^4 - 3x^3 + tx^2 - 4x + t - 1 = 0$$

has a rational root. *Ans.* $t = 1$.

70. For what values of t does the quadric surface

$$\frac{}{t+4} \quad \frac{y^2}{t+5} + \frac{}{t+8} \quad 1$$

pass through the point $(1, 1, -1)$? *Ans.* $t = -2, -6 \pm \sqrt{2}$.

71. Determine x and y so that

$$-4x + 13y + 5, \qquad 6x - 10y + 4, \qquad 2x + 8y - 2$$

are proportional to

$$y + 1, \qquad x + 1, \qquad x + y$$

respectively. *Ans.* $x = 3, y = 1; x = -\frac{3}{5}, y = -\frac{1}{5}; x = 3, y = -5.$

72. Show that the equation $x^3 - tx - t = 0$ has three distinct rational roots if, and only if, a rational number r exists such that

$$t = \frac{(3r^2 + 1)^3}{4r^2(r^2 - 1)^2};$$

and that when this condition is satisfied the three roots are

$$\frac{3r^2 + 1}{r^2 - 1}, \quad \frac{3r^2 + 1}{2r(r \pm 1)}$$

73. Show that the polynomial $x^{12} + ax^6 + 1$ is expressible as the product of two polynomials of degree 6 with rational coefficients if, and only if, $a = r + r^{-1}$, $a = 2 - r^2$, or $a = -2 - r^2$, where r is a rational number; and determine the factors in each case. (*American Mathematical Monthly*, (1936), p. 501.)

74. For what integral values of N is the polynomial $x^8 + Nx^4 + 1$ reducible in $R(1)$? (*American Mathematical Monthly*, (1935), p. 517.)

75. Show that if p is a prime number, the polynomial

$$(p - 1)x^{p-2} + (p - 2)x^{p-3} + \cdots + 2x + 1$$

is irreducible in $R(1)$.

76. Show that the polynomial

$$A_0(y)x^n + A_1(y)x^{n-1} + \cdots + A_{n-1}(y)x + A_n(y)$$

with coefficients in $R(y)$, where y is a variable, is irreducible in $R(y)$ if a polynomial $P(y)$, irreducible in R, exists which is a divisor of $A_1(y), \cdots, A_n(y)$ but not of $A_0(y)$, while $[P(y)]^2$ is not a divisor of $A_n(y)$. Illustrate. [Compare with Theorem 5, p. 66.]

77. Isolate the real roots of the equation

$$x^n - x^2 + x - 2 = 0, \qquad (n \geq 3).$$

78. Show that the equation

$$x^n + nax + b = 0, \qquad (n \text{ even})$$

with real coefficients has exactly two distinct real roots, one double root or no real roots according as

$$(n - 1)^{n-1}a^n - b^{n-1}$$

is positive, zero, or negative.

79. Show that the equation $3x^n - (x+1)^n - 1 = 0$ has a real root between $n/2$ and n.

80. Solve the equation $7^x + 8^x = 9^x$. *Ans.* $x = 3.9414 \cdots$.

81. Show that if a and b are positive numbers the equation $a^x + b^x = 1$ has

(a) no real root if one of the numbers a and b is ≤ 1 and the other is ≥ 1.

(b) exactly one real root if a and b are both < 1 or both > 1.

82. Show that if a, b, and c are positive numbers the equation $a^x + b^x = c$ has at most two real roots.

83. Show that t may be chosen sufficiently large so that the equation

$$x^4 - (2t+1)x^2 + t^2 + t - 1 = 0$$

has two roots whose difference is numerically less than any preassigned positive number.

84. The equations of the tangent line to the twisted cubic

$$x = t, \qquad y = t^2, \qquad z = t^3$$

are

$$\frac{x-t}{1} = \frac{y-t^2}{2t} = \frac{z-t^3}{3t^2}.$$

Find the equation of the surface generated by these tangent lines.

Ans. $4x^3z - 3x^2y^2 + 4y^3 - 6xyz + z^2 = 0$.

85. (a) Derive the *two-square identity*

$$(a^2+b^2)(c^2+d^2) = (ac-bd)^2 + (ad+bc)^2$$

from the identity

$$(a+bi)(c+di) = ac - bd + (ad+bc)i, \qquad (i = \sqrt{-1}.)$$

(b) Prove that a polynomial $f(x)$ with real coefficients which is ≥ 0 for every real x is expressible as the sum of the squares of two polynomials with real coefficients.

86. What is the length of the longest rectangle an inch wide that can be placed inside a rectangle 12 inches long by 8 inches wide?

Ans. 13.52 inches. (*American Mathematical Monthly*, (1916), p. 173.)

87. The roots of the equation

$$(1+t)z^3 - 1 + ti = 0$$

are, for every real $t \neq -1$, the vertices of an equilateral triangle in the $z = x + yi$-plane. Find the locus of these vertices as t varies through all real numbers. *Ans.* $x^3 + y^3 - 3x^2y - 3xy^2 = 1$.

88. Find the condition that the curve

$$y = a_0x^4 + 4a_1x^3 + 6a_2x^2 + 4a_3x + a_4, \qquad (a_0 \neq 0)$$

be symmetric with respect to a line parallel to the y-axis.

Ans. $a_0^2 - 3a_0a_1a_2 + 2a_1^3 = 0$.

89. What conditions must be satisfied by the coefficients of the cubic equation $x^3 - px^2 + qx - r = 0$ in order that its roots, considered as lengths, shall form a triangle. (*American Mathematical Monthly* (1925), p. 266.) [See p. 45, Ex. 16.]

90. Show that if all the roots of a polynomial $f(x)$ with real coefficients are real and distinct, then

$$[f'(x)]^2 > f(x)f''(x)$$

for every real x.

91. Let $f(x)$ be a polynomial in the field of complex numbers and M any positive number. Prove that a positive number P exists such that the absolute value of every root of the equation $f(x) = c$ exceeds M if $|c| > P$. In other words the absolute value of every root of the equation $f(x) = c$ tends to ∞ as $|c| \to \infty$.

92. Show that if $f(x)$ is a polynomial of degree ≥ 2 with real coefficients, the equation $f(x) = c$ (c real) has at most two real roots when $|c|$ is sufficiently large. Illustrate graphically.

93. Let ρ be a real root of odd multiplicity of a polynomial $F(x)$ with real coefficients. Prove that an interval $[a, b]$ containing ρ can be chosen so that

$$F'(a), \ F'(x), \ F'(b), \qquad (x \neq \rho, a < x < b)$$

have the same sign. Illustrate graphically.

94. Let $F(x)$ be a polynomial with real coefficients and positive leading coefficient. Prove that if a real number c exists such that $cF(x) - F'(x) \geq 0$ for every real x, then $F(x)$ has no real root and is positive for every real x.

95. Show that the polynomial

$$F(x) = 1 + x + \frac{x^2}{2!} + \cdots + \frac{x^n}{n!}$$

has no real root if n is even and exactly one real root if n is odd. [Observe that $F(x) - F'(x) = \frac{x^n}{n!}$.]

96. Show that if the polynomial $f(x)$, of degree n, is ≥ 0 for every real x, then the polynomial

$$F(x) = f(x) + f'(x) + f''(x) + \cdots + f^{(n)}(x)$$

is positive for every real x. (A. Hurwitz, *Mathematische Annalen* (1913), p. 173.)

97. Solve the equation $x^4 - 4x^3 - 4x + 1 = 0$ by radicals. Show that two of the roots are real and two imaginary, and that the two imaginary roots lie on the unit circle.

98. Show that if a root of a polynomial in the field of complex numbers

is on the unit circle, then the absolute value of each coefficient of the polynomial is $\leq$ the sum of the absolute values of the other coefficients.

99. Let s_k be the sum of the kth powers of the roots of a polynomial $f(x)$ in the field of complex numbers. Show that

$$\frac{f'(x)}{f(x)} = \frac{s_0}{x} + \frac{s_1}{x^2} + \frac{s_2}{x^3} + \cdots .$$

The series converges for every x whose absolute value exceeds the absolute values of the roots of $f(x)$.

100. Show that if a satisfies the inequalities

$$a \geq |a_1/a_0|,\ a \geq |a_2/a_0|, \cdots, a \geq |a_n/a_0|,$$

then the absolute value of each root of the equation

$$a_0z^n + a_1z^{n-1} + \cdots + a_{n-1}z + a_n = 0, \qquad (a_0 \neq 0)$$

is $< a + 1$.

101. Show that if M satisfies the inequalities

$$M \geq |na_1/a_0|,\ M \quad \sqrt{na_2/a_0}|, \cdots, M \geq |\sqrt[n]{na_n/a_0}|,$$

then the absolute value of each root of the equation of Ex. 100 is $\leq M$.

102. Show that the equation of Ex. 100 has at least one root whose

$-k\ |$

absolute value is $\leq$ $\qquad (a_0a_ka_n \neq 0;\ \ 0 \leq k < n).$

103. Let $f(z)$ be a polynomial of degree n in the field of complex numbers and λ an arbitrary complex number. Show that a circle of radius $|\lambda|$ whose center is a root of the equation $nf(z) - \lambda f'(z) = 0$ includes at least one root of $f(z)$.

104. Let $f(z)$ be a polynomial of degree n in the field of complex numbers, and let α be a root of $f(z)$ nearest a given point z. Prove that $|z - \alpha| \leq n\,|f(z)/f'(z)|$.

105. Let $f(z)$ be a polynomial of degree n in the field of complex numbers having distinct roots $z_1, \cdots, z_n$. Show that if

$$0 < M \leq |f'(z_k)|, \qquad (k = 1, \cdots, n),$$

then $|z - \alpha| \leq n\,|f(z)|\,/M$, where α is a root of $f(z)$ nearest a given point z.

106. Let $f(z)$ be a primary polynomial of degree n in the field of complex numbers. Show that if α is a root of $f(z)$ nearest a given point z and β a root farthest from z, then

$$|z - \alpha| \leq |\sqrt[n]{f(z)}| \leq |z - \beta|.$$

107. Show that if $r_1, r_2, \cdots, r_n$ are positive numbers, all the roots of the equation

$$(z + r_1)(z + r_2) \cdots (z + r_n) = \lambda(z - r_1)(z - r_2) \cdots (z - r_n),\ |\lambda| = 1,$$

are on the axis of pure imaginary numbers.

108. Show that if $b_1, \cdots, b_n$ are positive numbers, all the roots of the equation

$$(z - a_1 - b_1 i) \cdots (z - a_n - b_n i) = \lambda(z - a_1 + b_1 i) \cdots (z - a_n + b_n i),$$
$$|\lambda| = 1,$$

are real. Here $a_1, \cdots, a_n$ are real numbers.

109. Show that if the equation

$$a_0 z^n + a_1 z^{n-1} + \cdots + a_{n-1} z + a_n = 0$$

has real coefficients but no real roots, then the curve

$$a_0 x^n + a_1 x^{n-1} y + \cdots + a_{n-1} x y^{n-1} + a_n y^n = a$$

where a is an arbitrary real number, has no infinite branch.

110. If a field includes one of two conjugate imaginary numbers, does it necessarily include the other?

111. The equation $x^5 + 4x^4 + 2x^3 - 13x^2 - 19x - 5 = 0$ has two roots of the form $a + bi$, where a and b are integers. Find them.

112. Show that if n is a positive integer, there exists a polynomial $P_n(x)$ of degree n, with integral coefficients, such that

$$\cos n\theta = P_n(\cos \theta).$$

113. Show that $\cos 1°$ and $\sin 1°$ are algebraic numbers.

114. Show that it is impossible, with ruler and compasses, to construct a triangle, given the perimeter and the radii of the inscribed and circumscribed circles. (*American Mathematical Monthly* (1924), p. 502.)

115. Show that it is impossible, with ruler and compasses, to draw a line through a given point intersecting a given line and a given circle so that the part of the line between the given point and the given line equals the part within the circle. (*American Mathematical Monthly* (1925), p. 482; (1926), p. 106.)

INDEX

The numbers refer to pages